Atty. Dkt. No. 053969-0157

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Masanao SAKAI

Title: NETWORK, IPsec SETTING SERVER APPARATUS, IPsec PROCESSING APPARATUS, AND IPsec SETTING METHOD USED THEREFOR

Appl. No.: Unassigned

Filing Date: 09/05/2003

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

Japanese Patent Application No. 2002-264913
filed 09/11/2002.

Respectfully submitted,

Reg No. 34,717

Date: September 5, 2003

By _____
for David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

FOLEY & LARDNER
Customer Number: 22428

22428
PATENT TRADEMARK OFFICE
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００２年　９月１１日

出　願　番　号
Application Number:　特願２００２－２６４９１３

[ST. 10/C]:　［ＪＰ２００２－２６４９１３］

出　願　人
Applicant(s):　日本電気株式会社

２００３年　８月１２日

特許庁長官
Commissioner,
Japan Patent Office　今井康夫

出証番号　出証特２００３－３０６４７６１

【書類名】　特許願
【整理番号】　41810227
【提出日】　平成14年 9月11日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　酒井　征直
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100088812
【弁理士】
【氏名又は名称】　▲柳▼川　信
【手数料の表示】
【予納台帳番号】　030982
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9001833
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　ネットワーク、ＩＰｓｅｃ設定サーバ装置、ＩＰｓｅｃ処理装置及びそれらに用いるＩＰｓｅｃ設定方法

【特許請求の範囲】

【請求項１】　異なる２つの拠点間をインタネットを介して通信する場合にインタネット経路上でのセキュリティを確保するためのＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置と、前記ＩＰｓｅｃ処理装置のＩＰｓｅｃ設定を管理するＩＰｓｅｃ設定サーバ装置とを含むネットワークであって、第１及び第２のＩＰｓｅｃ処理装置間に適用する前記ＩＰｓｅｃのポリシーを一括管理する機能を前記ＩＰｓｅｃ設定サーバ装置に有することを特徴とするネットワーク。

【請求項２】　前記第１のＩＰｓｅｃ処理装置から受信した前記第２のＩＰｓｅｃ処理装置との間の通信に対する要求メッセージの内容を基に前記第２のＩＰｓｅｃ処理装置との間に適用する前記ＩＰｓｅｃのポリシーを特定する機能を前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項１記載のネットワーク。

【請求項３】　前記要求メッセージを受信した場合に当該要求メッセージを送信した前記第１のＩＰｓｅｃ処理装置の通信相手である前記第２のＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２記載のネットワーク。

【請求項４】　前記要求起動メッセージに対する応答がない時に前記第１のＩＰｓｅｃ処理装置に対して前記第２のＩＰｓｅｃ処理装置からの応答なしを通知する機能を前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項３記載のネットワーク。

【請求項５】　前記要求メッセージの内容とそれに適用する前記ＩＰｓｅｃのポリシーの内容とから当該ＩＰｓｅｃ通信に必要となるＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）パラメータを生成する機能を前記ＩＰｓｅｃ設定

サーバ装置に含むことを特徴とする請求項２から請求項４のいずれか記載のネットワーク。

【請求項６】　前記要求メッセージに対して前記ＩＰｓｅｃのポリシーと前記ＳＡパラメータとを少なくとも含む配布メッセージを送信する機能を前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２から請求項５のいずれか記載のネットワーク。

【請求項７】　前記ＩＰｓｅｃの暗号化及び認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記ＩＰｓｅｃ処理装置に配布する機能とを前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項１から請求項６のいずれか記載のネットワーク。

【請求項８】　異なる２つの拠点間をインタネットを介して通信する場合にインタネット経路上でのセキュリティを確保するためのＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置のＩＰｓｅｃ設定を管理するＩＰｓｅｃ設定サーバ装置であって、前記ＩＰｓｅｃ処理装置間に適用する前記ＩＰｓｅｃのポリシーを一括管理する機能を有することを特徴とするＩＰｓｅｃ設定サーバ装置。

【請求項９】　前記ＩＰｓｅｃ処理装置から受信した他のＩＰｓｅｃ処理装置との間の通信に対する要求メッセージの内容を基に前記他のＩＰｓｅｃ処理装置との間に適用する前記ＩＰｓｅｃのポリシーを特定する機能を含むことを特徴とする請求項８記載のＩＰｓｅｃ設定サーバ装置。

【請求項１０】　前記要求メッセージを受信した場合に当該要求メッセージを送信したＩＰｓｅｃ処理装置の通信相手のＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を含むことを特徴とする請求項９記載のＩＰｓｅｃ設定サーバ装置。

【請求項１１】　前記要求起動メッセージに対する応答がない時に前記要求メッセージを送信したＩＰｓｅｃ処理装置に対して前記通信相手のＩＰｓｅｃ処理装置からの応答なしを通知する機能を含むことを特徴とする請求項１０記載の前記ＩＰｓｅｃ設定サーバ装置。

【請求項１２】　前記要求メッセージの内容とそれに適用する前記ＩＰｓｅ

ｃのポリシーの内容とから当該ＩＰｓｅｃ通信に必要となるＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）パラメータを生成する機能を含むことを特徴とする請求項９から請求項１１のいずれか記載のＩＰｓｅｃ設定サーバ装置。

【請求項１３】　前記要求メッセージに対して前記ＩＰｓｅｃのポリシーと前記ＳＡパラメータとを少なくとも含む配布メッセージを送信する機能を含むことを特徴とする請求項９から請求項１２のいずれか記載のＩＰｓｅｃ設定サーバ装置。

【請求項１４】　前記ＩＰｓｅｃの暗号化や認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記ＩＰｓｅｃ処理装置に配布する機能とを含むことを特徴とする請求項８から請求項１３のいずれか記載のＩＰｓｅｃ設定サーバ装置。

【請求項１５】　インタネットにおいてＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置であって、前記ＩＰｓｅｃを適用すべきパケットを受信した場合にＩＰｓｅｃ設定サーバ装置で一括管理される当該ＩＰｓｅｃに関する設定を前記ＩＰｓｅｃ設定サーバ装置に問い合わせるか否かを判断する機能を有することを特徴とするＩＰｓｅｃ処理装置。

【請求項１６】　前記ＩＰｓｅｃに関する設定を取得するために前記ＩＰｓｅｃ設定サーバ装置に他のＩＰｓｅｃ処理装置との間の通信に対する要求メッセージを送信する機能を含むことを特徴とする請求項１５記載のＩＰｓｅｃ処理装置。

【請求項１７】　前記ＩＰｓｅｃ設定サーバ装置から前記要求メッセージを送信させるための要求起動メッセージを受信した時に当該要求メッセージの送信を行うことを特徴とする請求項１６記載のＩＰｓｅｃ処理装置。

【請求項１８】　前記ＩＰｓｅｃ設定サーバ装置から受信した配布メッセージを基に前記ＩＰｓｅｃを適用するためのポリシーを記録するＳＰＤ及び個々の通信に対して前記ＩＰｓｅｃの処理を実施するために必要なＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）を記録するＳＡＤを設定する機能を含むことを特徴とする請求項１５から請求項１７のいずれか記載のＩＰｓｅｃ処理装置。

【請求項１９】　前記ＩＰｓｅｃの暗号化や認証に使用するための共有秘密鍵を前記ＩＰｓｅｃ設定サーバ装置から取得する機能を含むことを特徴とする請求項１５から請求項１８のいずれか記載のＩＰｓｅｃ処理装置。

【請求項２０】　前記ＳＡの有効期限が満了する前に前記ＩＰｓｅｃ設定サーバ装置に前記要求メッセージを再送信して新しい設定情報を取得する機能を含むことを特徴とする請求項１５から請求項１９のいずれか記載のＩＰｓｅｃ処理装置。

【請求項２１】　異なる２つの拠点間をインタネットを介して通信する場合にインタネット経路上でのセキュリティを確保するためのＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置と、前記ＩＰｓｅｃ処理装置のＩＰｓｅｃ設定を管理するＩＰｓｅｃ設定サーバ装置とからなるネットワークのＩＰｓｅｃ設定方法であって、前記ＩＰｓｅｃ処理装置間に適用する前記ＩＰｓｅｃのポリシーを一括管理するステップを前記ＩＰｓｅｃ設定サーバ装置に有することを特徴とするＩＰｓｅｃ設定方法。

【請求項２２】　前記ＩＰｓｅｃ処理装置から受信した他のＩＰｓｅｃ処理装置との間の通信に対する要求メッセージの内容を基に前記他のＩＰｓｅｃ処理装置との間に適用する前記ＩＰｓｅｃのポリシーを特定するステップを前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２１記載のＩＰｓｅｃ設定方法。

【請求項２３】　前記要求メッセージを受信した場合に当該要求メッセージを送信したＩＰｓｅｃ処理装置の通信相手のＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信するステップを前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２２記載のＩＰｓｅｃ設定方法。

【請求項２４】　前記要求起動メッセージに対する応答がない時に前記要求メッセージを送信したＩＰｓｅｃ処理装置に対して前記通信相手のＩＰｓｅｃ処理装置からの応答なしを通知する機能を前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２３記載のＩＰｓｅｃ設定方法。

【請求項２５】　前記要求メッセージの内容とそれに適用する前記ＩＰｓｅｃのポリシーの内容とから当該ＩＰｓｅｃ通信に必要となるＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）パラメータを生成するステップを前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２２または請求項２４記載のＩＰｓｅｃ設定方法。

【請求項２６】　前記要求メッセージに対して前記ＩＰｓｅｃのポリシーと前記ＳＡパラメータとを少なくとも含む配布メッセージを送信するステップを前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２２から請求項２５のいずれか記載のＩＰｓｅｃ設定方法。

【請求項２７】　前記ＩＰｓｅｃの暗号化や認証に使用するための共有秘密鍵を生成するステップと、その生成した前記共有秘密鍵を前記ＩＰｓｅｃ処理装置に配布するステップとを前記ＩＰｓｅｃ設定サーバ装置に含むことを特徴とする請求項２１から請求項２６のいずれか記載のＩＰｓｅｃ設定方法。

【請求項２８】　前記ＩＰｓｅｃ処理装置が、前記ＩＰｓｅｃを適用すべきパケットを受信した場合にＩＰｓｅｃ設定サーバ装置で一括管理される当該ＩＰｓｅｃに関する設定を前記ＩＰｓｅｃ設定サーバ装置に問い合わせるか否かを判断することを特徴とする請求項２１から請求項２７のいずれか記載のＩＰｓｅｃ設定方法。

【請求項２９】　前記ＩＰｓｅｃ処理装置が、前記ＩＰｓｅｃに関する設定を取得するために前記ＩＰｓｅｃ設定サーバ装置に他のＩＰｓｅｃ処理装置との間の通信に対する要求メッセージを送信することを特徴とする請求項２１から請求項２８のいずれか記載のＩＰｓｅｃ設定方法。

【請求項３０】　前記ＩＰｓｅｃ処理装置が、前記ＩＰｓｅｃ設定サーバ装置から受信した配布メッセージを基に前記ＩＰｓｅｃを適用するためのポリシーを記録するＳＰＤ及び個々の通信に対して前記ＩＰｓｅｃの処理を実施するために必要なＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）を記録するＳＡＤを設定することを特徴とする請求項２１から請求項２９のいずれか記載のＩＰｓｅｃ設定方法。

【請求項３１】　前記ＩＰｓｅｃ処理装置が、前記ＩＰｓｅｃの暗号化や認

証に使用するための共有秘密鍵を前記ＩＰｓｅｃ設定サーバ装置から取得することを特徴とする請求項２１から請求項３０のいずれか記載のＩＰｓｅｃ設定方法。

【請求項３２】　前記ＩＰｓｅｃ処理装置が、前記ＳＡの有効期限が満了する前に前記ＩＰｓｅｃ設定サーバ装置に前記要求メッセージを再送信して新しい設定情報を取得することを特徴とする請求項２１から請求項３１のいずれか記載のＩＰｓｅｃ設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はネットワーク、ＩＰｓｅｃ設定サーバ装置、ＩＰｓｅｃ処理装置及びそれらに用いるＩＰｓｅｃ設定方法に関し、特にインタネット上で機密性、完全性、認証等の機能を提供するＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）によるネットワーク構成に関する。

【０００２】

【従来の技術】

従来、インタネットの普及に伴って、インタネット上でのセキュリティを確保したいという要望が高まっている。特に、多くの企業においては、高価な専用線を用いてネットワークを構築する代わりに、インタネット上に仮想的な私設網を構築し、遠隔地のオフィス等を結ぶネットワークを安価に構築したいという要望も多い。

【０００３】

このような要望に対して、インタネット上で機密性、完全性、認証等の機能を提供するＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）がＩＥＴＦ（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）によって標準化されている（例えば、特許文献１参照）。

【０００４】

ＩＰｓｅｃを用いることによって、異なる２つの拠点間をインタネットを介し

て通信する場合には、インタネット経路上でのセキュリティを確保することが可能となる。新しいインタネットプロトコルであるＩＰｖ６（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ ｖｅｒｓｉｏｎ ６）ではＩＰｓｅｃのサポートが必須となり、今後、ますます多くのネットワーク機器がＩＰｓｅｃに対応し、ＩＰｓｅｃを使用した通信もますます増えることが予想される。

【０００５】

このＩＰｓｅｃを使用した通信を行うＩＰｓｅｃ処理装置の構成を図３１に示す。図３１において、ＩＰｓｅｃ処理装置４はインタフェース部（Ｉ／Ｆ）４１，４２と、ＩＰｓｅｃ処理部４３と、ＳＰＤ（Ｓｅｃｕｒｉｔｙ Ｐｏｌｉｃｙ Ｄａｔａｂａｓｅ）４４と、ＳＡＤ（Ｓｅｃｕｒｉｔｙ Ａｓｓｏｃｉａｔｉｏｎ Ｄａｔａｂａｓｅ）４５と、ルーティング部４６とを具備している。

【０００６】

インタフェース部４１はプライベートネットワークに接続され、プライベートネットワークとのデータ通信を行う。インタフェース部４２はインタネットに接続され、インタネットを介したデータ通信を行う。

【０００７】

ＩＰｓｅｃ処理部４３はインタフェース部４１，４２から受信したデータ通信パケットに対してＩＰｓｅｃ処理を実施する。ＳＰＤ４４はＩＰｓｅｃ処理部４３から参照され、ＩＰｓｅｃを適用するためのポリシーが記録されている。ＳＡＤ４５はＩＰｓｅｃ処理部４３から参照され、個々の通信に対してＩＰｓｅｃ処理を実施するために必要なＳＡが記録されている。ルーティング部４６はＩＰｓｅｃ処理部４３との間でデータ通信パケットの送受信を行い、各々のデータ通信パケットの転送先を決定する。

【０００８】

特開２００１－２９８４４９号公報（第８－１１頁、図１）

【０００９】

【発明が解決しようとする課題】

しかしながら、上述した従来のＩＰｓｅｃによるネットワーク構成では、１台のＩＰｓｅｃ処理装置が多くの相手とＩＰｓｅｃ通信を実施する場合、ＩＰｓｅ

ｃによる接続において、ＩＰｓｅｃ処理を実施する装置に設定する内容が多いという問題がある。

【００１０】

ＩＰｓｅｃを利用するためには、ＩＰｓｅｃを適用する通信に対して使用するサービス［ＡＨ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｈｅａｄｅｒ：認証ヘッダ），ＥＳＰ（Ｅｎｃａｐｓｕｌａｔｉｎｇ　Ｓｅｃｕｒｉｔｙ　Ｐａｙｌｏａｄ：カプセル化セキュリティペイロード）によって提供されるサービス］、使用するアルゴリズム等を、ＩＰｓｅｃ処理を実施する両端の装置にそれぞれ設定する必要がある。

【００１１】

自動鍵管理プロトコル（ＩＫＥ：Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）を使用する場合には、自動鍵管理プロトコルで利用される暗号化アルゴリズム、ハッシュアルゴリズム、鍵共有アルゴリズム等も両端の装置に設定する必要がある。これらの設定の数はＩＰｓｅｃによって接続する相手毎に必要となるため、ＩＰｓｅｃによって接続する相手が多くなるほど、多くの設定が必要となる。

【００１２】

また、従来のＩＰｓｅｃによるネットワーク構成では、ＩＰｓｅｃを適用する通信の両端で異なる設定をしてしまう可能性があるという問題がある。ＩＰｓｅｃ処理を実施する両端の装置において、使用するサービスの設定や、使用するアルゴリズムの設定に異なる設定をしてしまった場合、通信することができなくなる。ＩＰｓｅｃを適用する通信が多くなると、設定の数も多くなるため、このような間違いが発生する可能性も増える。

【００１３】

さらに、従来のＩＰｓｅｃによるネットワーク構成では、自動鍵管理プロトコルを使用した場合に、共有秘密鍵を生成する演算に時間がかかり、結果として通信を開始することができるまでに時間がかかるという問題がある。通常、ＩＰｓｅｃ処理装置では、図３２に示すように、当該通信が必要になった時点で初めて共有秘密鍵の生成を始めるため、共有秘密鍵の生成に時間がかかれば、通信開

始までに時間がかかってしまう。

【００１４】

さらにまた、従来のＩＰｓｅｃによるネットワーク構成では、自動鍵管理プロトコルを使用した場合に、ＩＰｓｅｃ処理を実施する装置に演算負荷が発生するという問題がある。共有秘密鍵を生成するためには多くの演算が必要となり、当該装置の持つ他の機能（ＩＰｓｅｃを適用しないパケットの転送機能等）の性能が低下してしまう。同時に扱うＩＰｓｅｃ通信が多くなると、共有秘密鍵を生成する機会も多くなり、性能が低下する割合も多くなる。

【００１５】

そこで、本発明の目的は上記の問題点を解消し、通信する装置間での設定不一致を防止することができるネットワーク、ＩＰｓｅｃ設定サーバ装置、ＩＰｓｅｃ処理装置及びそれらに用いるＩＰｓｅｃ設定方法を提供することにある。

【００１６】

また、本発明の他の目的は、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信元からのパケットを取りこぼしなく受取ることができるネットワーク、ＩＰｓｅｃ設定サーバ装置、ＩＰｓｅｃ処理装置及びそれらに用いるＩＰｓｅｃ設定方法を提供することにある。

【００１７】

また、本発明の別の目的は、秘密鍵演算を不要とし、個々の装置での通信開始時のＩＰｓｅｃ経路の接続時間を短縮することができ、性能の低下を防ぐことができるネットワーク、ＩＰｓｅｃ設定サーバ装置、ＩＰｓｅｃ処理装置及びそれらに用いるＩＰｓｅｃ設定方法を提供することにある。

【００１８】

【課題を解決するための手段】

本発明によるネットワークは、異なる２つの拠点間をインタネットを介して通信する場合にインタネット経路上でのセキュリティを確保するためのＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置と、前記ＩＰｓｅｃ処理装置のＩＰｓｅｃ設定を管理するＩＰｓｅｃ設定サーバ装置とを含むネットワークであって、前記ＩＰ

ｓｅｃ処理装置間に適用する前記ＩＰｓｅｃのポリシーを一括管理する機能を前記ＩＰｓｅｃ設定サーバ装置に備えている。

【００１９】

本発明による他のネットワークは、上記の構成のほかに、前記要求メッセージを受信した場合に当該要求メッセージを送信したＩＰｓｅｃ処理装置の通信相手のＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を前記ＩＰｓｅｃ設定サーバ装置に具備している。

【００２０】

本発明による別のネットワークは、上記の構成のほかに、前記ＩＰｓｅｃの暗号化及び認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記ＩＰｓｅｃ処理装置に配布する機能とを前記ＩＰｓｅｃ設定サーバ装置に具備している。

【００２１】

本発明によるＩＰｓｅｃ設定サーバ装置は、異なる２つの拠点間をインタネットを介して通信する場合にインタネット経路上でのセキュリティを確保するためのＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置のＩＰｓｅｃ設定を管理するＩＰｓｅｃ設定サーバ装置であって、前記ＩＰｓｅｃ処理装置間に適用する前記ＩＰｓｅｃのポリシーを一括管理する機能を備えている。

【００２２】

本発明による他のＩＰｓｅｃ設定サーバ装置は、上記の構成のほかに、前記要求メッセージを受信した場合に当該要求メッセージを送信したＩＰｓｅｃ処理装置の通信相手のＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信する機能を具備している。

【００２３】

本発明による別のＩＰｓｅｃ設定サーバ装置は、上記の構成のほかに、前記ＩＰｓｅｃの暗号化や認証に使用するための共有秘密鍵を生成する機能と、その生成した前記共有秘密鍵を前記ＩＰｓｅｃ処理装置に配布する機能とを具備してい

る。

【００２４】

本発明によるＩＰｓｅｃ処理装置は、インタネットにおいてＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置であって、前記ＩＰｓｅｃを適用すべきパケットを受信した場合にＩＰｓｅｃ設定サーバ装置で一括管理される当該ＩＰｓｅｃに関する設定を前記ＩＰｓｅｃ設定サーバ装置に問い合わせるか否かを判断する機能を備えている。

【００２５】

本発明による他のＩＰｓｅｃ処理装置は、上記の構成において、前記ＩＰｓｅｃ設定サーバ装置から前記要求メッセージを送信させるための要求起動メッセージを受信した時に当該要求メッセージの送信を行っている。

【００２６】

本発明による別のＩＰｓｅｃ処理装置は、上記の構成のほかに、前記ＩＰｓｅｃの暗号化や認証に使用するための共有秘密鍵を前記ＩＰｓｅｃ設定サーバ装置から取得する機能を具備している。

【００２７】

本発明によるＩＰｓｅｃ設定方法は、異なる２つの拠点間をインタネットを介して通信する場合にインタネット経路上でのセキュリティを確保するためのＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置と、前記ＩＰｓｅｃ処理装置のＩＰｓｅｃ設定を管理するＩＰｓｅｃ設定サーバ装置とからなるネットワークのＩＰｓｅｃ設定方法であって、前記ＩＰｓｅｃ処理装置間に適用する前記ＩＰｓｅｃのポリシーを一括管理するステップを前記ＩＰｓｅｃ設定サーバ装置に備えている。

【００２８】

本発明による他のＩＰｓｅｃ設定方法は、上記の動作において、前記要求メッセージを受信した場合に当該要求メッセージを送信したＩＰｓｅｃ処理装置の通信相手のＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信するステップを前記ＩＰｓｅｃ設定サーバ装置

に具備している。

【００２９】

本発明による別のＩＰｓｅｃ設定方法は、上記のステップのほかに、前記ＩＰｓｅｃの暗号化や認証に使用するための共有秘密鍵を生成するステップと、その生成した前記共有秘密鍵を前記ＩＰｓｅｃ処理装置に配布するステップとを前記ＩＰｓｅｃ設定サーバ装置に具備している。

【００３０】

すなわち、本発明のＩＰｓｅｃ設定方法は、インタネットにおいてＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔｙ　ｐｒｏｔｏｃｏｌ）を使用するＩＰｓｅｃ処理装置において、個々のＩＰｓｅｃ処理装置に設定するポリシーをＩＰｓｅｃ設定サーバに一括して登録することによって、個々のＩＰｓｅｃ処理装置に設定するポリシーの数を削減するものである。

【００３１】

また、本発明のＩＰｓｅｃ設定方法では、上記構成において、要求メッセージを受信した場合に当該要求メッセージを送信したＩＰｓｅｃ処理装置の通信相手のＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信することによって、各ＩＰｓｅｃ処理装置間に適用するＩＰｓｅｃのポリシーの設定がそれらの装置でほぼ同時に行われることとなり、ポリシー設定後の暗号化や復号を滞りなく行うことが可能となる。これによって、送信先のＩＰｓｅｃ処理装置において送信元からのパケットを取りこぼしなく受取ることが可能となる。

【００３２】

さらに、本発明のＩＰｓｅｃ設定方法では、上記構成において、ＩＰｓｅｃ設定サーバが要求起動メッセージの送信時にそれに応答した要求メッセージを受信しなければ、送信元のＩＰｓｅｃ処理装置に応答なしエラーメッセージを送信するので、送信元のＩＰｓｅｃ処理装置で対向装置の不存在を認識することが可能となる。

【００３３】

さらにまた、本発明のＩＰｓｅｃ設定方法は、上記構成において、ＩＰｓｅｃ

の暗号化や認証に使用するための共有秘密鍵を各ＩＰｓｅｃ処理装置がＩＰｓｅｃ設定サーバから取得することによって、複雑な鍵交換演算を省略し、ＩＰｓｅｃ処理開始までの時間を短縮するものである。

【００３４】

より具体的に説明すると、本発明のＩＰｓｅｃ設定方法では、ＩＰｓｅｃ設定サーバが各ＩＰｓｅｃ処理装置間に適用するＩＰｓｅｃのポリシーを記憶している。送信元のＩＰｓｅｃ処理装置が相手先のＩＰｓｅｃ処理装置にデータ通信パケットを送信する場合、送信元のＩＰｓｅｃ処理装置は必要な設定をＩＰｓｅｃ設定サーバに要求する。要求を受信したＩＰｓｅｃ設定サーバは相手先のＩＰｓｅｃ処理装置に対しても設定を要求するように指示する。

【００３５】

相手先のＩＰｓｅｃ処理装置からの要求を受信した時点で、ＩＰｓｅｃ設定サーバは登録済みのポリシーと、送信元及び相手先の両方のＩＰｓｅｃ処理装置から通知されたＳＰＩ（Ｓｅｃｕｒｉｔｙ　Ｐａｒａｍｅｔｅｒｓ　Ｉｎｄｅｘ：セキュリティパラメータインデックス）、及びＩＰｓｅｃ設定サーバが生成した共有秘密鍵をそれぞれのＩＰｓｅｃ処理装置に送信する。この時点で送信元及び相手先の両方のＩＰｓｅｃ処理装置にはＩＰｓｅｃ処理に必要な情報がすべて揃い、ＩＰｓｅｃ処理を実行することが可能となる。尚、設定情報の送受信については、従来のＩＰｓｅｃによって保護することによって、第３者による盗聴を防ぐ。

【００３６】

このように、本発明では、ＩＰｓｅｃポリシーをＩＰｓｅｃ設定サーバで一括して管理することによって、全体の設定数を削減すると同時に、２拠点間での設定内容が異なるために発生する通信障害を防止することが可能となる。

【００３７】

また、本発明では、要求起動メッセージを送信しているので、要求メッセージの送信元のＩＰｓｅｃ処理装置に対向するＩＰｓｅｃ処理装置ではその送信元のＩＰｓｅｃ処理装置でのＩＰｓｅｃのポリシーの設定とほぼ同時にＩＰｓｅｃのポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元のＩＰ

ｓｅｃ処理装置がパケットを暗号化して送信すると、対向するＩＰｓｅｃ処理装置では送信元のＩＰｓｅｃ処理装置からのパケットを復号して受取ることが可能となる。これによって、送信先のＩＰｓｅｃ処理装置において送信元からのパケットを取りこぼしなく受取ることが可能となる。

【００３８】

さらに、本発明では、要求起動メッセージの送信時にそれに応答した要求メッセージが対向するＩＰｓｅｃ処理装置から送られてこなければ、送信元のＩＰｓｅｃ処理装置に対して応答なしエラーメッセージが送信されるので、送信元のＩＰｓｅｃ処理装置で対向装置の不存在を即座に認識することが可能となる。

【００３９】

さらにまた、本発明では、共有秘密鍵の取得にＩＫＥ（Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ：自動鍵管理プロトコル）を用いないため、ＩＫＥで使用するＤｉｆｆｉｅ－Ｈｅｌｌｍａｎの演算をする必要がない。したがって、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの演算を必要とする従来の手法と比較して、ＩＰｓｅｃ処理開始までの時間を短縮することが可能となる。

【００４０】

従来の手法ではＩＫＥのＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）を更新するためにＤｉｆｆｉｅ－Ｈｅｌｌｍａｎの演算が定期的に発生し、そのたびに演算負荷が発生する。ＩＰｓｅｃによる通信相手が多いほど、ＩＫＥのＳＡを更新する機会も増えるので、演算負荷も増加し、ＩＰｓｅｃ処理装置全体の処理性能が低下する。

【００４１】

これに対し、本発明では、ＩＰｓｅｃ処理装置とＩＰｓｅｃ設定サーバとの間以外の通信については、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの演算を行わないため、従来の手法と比較して、演算負荷も軽減することが可能となる。

【００４２】

【発明の実施の形態】

次に、本発明の実施例について図面を参照して説明する。図１は本発明の一実施例によるＩＰｓｅｃ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　ｓｅｃｕｒｉｔ

ｙ　ｐｒｏｔｏｃｏｌ）によるネットワークの構成を示すブロック図である。図１において、本発明の一実施例によるネットワークは互いにＩＰｓｅｃ適用通信を実施しようとする複数台のＩＰｓｅｃ処理装置２ａ～２ｆがインタネット１００を介して接続され、同じくインタネット１００上にＩＰｓｅｃ設定サーバ１を接続して構成している。尚、図１に示すように、ＩＰｓｅｃ処理装置２ａ～２ｆはそれぞれの背後に存在するプライベートネットワーク２０１～２０４をＩＰｓｅｃによる通信によって相互に接続するルータであってもよいし、自分自身の通信にＩＰｓｅｃを適用するパーソナルコンピュータ（以下、パソコンとする）であってもよい。

【００４３】

図２に図１のＩＰｓｅｃ設定サーバ１の構成を示すブロック図である。図２において、ＩＰｓｅｃ設定サーバ１はインタフェース（Ｉ／Ｆ）部１１と、ＩＰｓｅｃ処理部１２と、ＳＰＤ（Ｓｅｃｕｒｉｔｙ　Ｐｏｌｉｃｙ　Ｄａｔａｂａｓｅ）１３と、ＳＡＤ　（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ　Ｄａｔａｂａｓｅ）１４と、要求処理部１５と、配布ポリシー記憶部１６と、管理テーブル１７と、乱数生成器１８と、タイマ１９と、記録媒体２０とから構成されている。ここで、ＩＰｓｅｃ設定サーバ１は主にコンピュータから構成され、コンピュータが記録媒体２０に格納されたプログラムを実行することで上記の各部の動作が実現される。

【００４４】

インタフェース部１１はインタネット１００に接続され、インタネット１００を介したデータ通信を行う。ＩＰｓｅｃ処理部１２はインタフェース部１１から受信したデータ通信パケットに対してＩＰｓｅｃ処理を実施する。

【００４５】

ＳＰＤ１３はＩＰｓｅｃ処理部１２から参照され、ＩＰｓｅｃを適用するためのポリシーを記録している。ＳＡＤ１４はＩＰｓｅｃ処理部１２から参照され、個々の通信に対してＩＰｓｅｃ処理を実施するために必要なＳＡ（Ｓｅｃｕｒｉｔｙ　Ａｓｓｏｃｉａｔｉｏｎ）を記録している。

【００４６】

要求処理部１５はインタフェース部１１経由でＩＰｓｅｃ処理装置２ａ～２ｆから設定要求メッセージを受信し、配布メッセージを返す。配布ポリシー記憶部１６は要求処理部１５から参照され、要求された設定を決定するために必要なＩＰｓｅｃポリシーが記憶されている。管理テーブル１７は要求処理部１５から参照、設定され、設定要求を受けた各々のＳＡ通信に関する情報が記憶されている。

【００４７】

乱数生成器１８は要求処理部１５からの要求によって乱数を生成する。タイマ１９は要求処理部１５から要求され、時間を計測する。これらの中でＩＰｓｅｃ処理部１２、ＳＡＤ１４、ＳＰＤ１３はＩＰｓｅｃ設定サーバ１がＩＰｓｅｃ処理装置２との通信をＩＰｓｅｃによって保護するために必要となるだけであり、従来のＩＰｓｅｃの機構と同一である。

【００４８】

インタフェース部１１はインタネット１００からデータ通信パケットを受信すると、そのデータ通信パケットをＩＰｓｅｃ処理部１２に転送し、またＩＰｓｅｃ処理部１２から転送されたデータ通信パケットをインタネット１００に送信する。

【００４９】

ＩＰｓｅｃ処理部１２はインタネット１００から受信したＩＰｓｅｃ適用済みのデータ通信パケットに対してＳＡＤ１４やＳＰＤ１３の記憶内容を基にＩＰｓｅｃの復号処理を行い、ＩＰｓｅｃ適用前の状態にして要求処理部１５に転送する。また、ＩＰｓｅｃ処理部１２は要求処理部１５から受信したデータ通信パケットに対してＳＰＤ１３及びＳＡＤ１４の記憶内容にしたがってＩＰｓｅｃ処理を適用し、インタフェース部１１に転送する。ＩＰｓｅｃ処理部１２はＩＰｓｅｃ設定サーバ１とＩＰｓｅｃ処理装置２ａ～２ｆとの間の通信を保護するために必要な機構であり、従来のＩＰｓｅｃと全く同じものである。

【００５０】

図３は図２の配布ポリシー記憶部１６の記憶内容を示す図である。図３において、配布ポリシー記憶部１６には配布ポリシーを特定するためのアドレスペア欄

と、配布するＩＰｓｅｃポリシーを設定する配布ポリシー欄とがある。配布ポリシー記憶部１６の配布ポリシーに設定可能なパラメータはＩＰｓｅｃプロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、ＳＡの有効期間である。

【００５１】

図３に示す例では、ＩＰｓｅｃ処理装置２ａ－ＩＰｓｅｃ処理装置２ｂ間の通信に適用するＩＰｓｅｃポリシー、ＩＰｓｅｃ処理装置２ｄ－ＩＰｓｅｃ処理装置２ｅ間の通信に適用するＩＰｓｅｃポリシーが設定されている。尚、配布ポリシー記憶部１６には予めすべての項目をユーザが設定しておく必要がある。また、一度設定した後は動作中に自動的に書換えられることはない。

【００５２】

ＩＰｓｅｃ処理装置２ａ－ＩＰｓｅｃ処理装置２ｂ間の配布ポリシーとしては、ＩＰｓｅｃプロトコルに「ＥＳＰ（Ｅｎｃａｐｓｕｌａｔｉｎｇ　Ｓｅｃｕｒｉｔｙ　Ｐａｙｌｏａｄ：カプセル化セキュリティペイロード）」、カプセル化モードに「トンネルモード」、暗号化アルゴリズムに「ＤＥＳ－ＣＢＣ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ－Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）」、認証アルゴリズムに「ＨＭＡＣ（Ｈａｓｈｉｎｇ　Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｃｏｄｅ）－ＭＤ５－９６」、ＳＡの有効期間に「３６００秒」が設定されている。

【００５３】

また、ＩＰｓｅｃ処理装置２ｄ－ＩＰｓｅｃ処理装置２ｅ間の配布ポリシーとしては、ＩＰｓｅｃプロトコルに「ＥＳＰ」、カプセル化モードに「トランスポートモード」、暗号化アルゴリズムに「３ＤＥＳ－ＣＢＣ」、認証アルゴリズムに「ＨＭＡＣ－ＳＨＡ－１－９６」、ＳＡの有効期間に「３６００秒」が設定されている。

【００５４】

従来の手法では適用するＩＰｓｅｃポリシーの内容についてそれぞれのＩＰｓｅｃ処理装置２ａ～２ｆに個別に同一の設定を入力する必要があるが、本発明の手法ではＩＰｓｅｃ処理装置２ａ～２ｆ間のＩＰｓｅｃ通信に対しては配布ポリ

シー記憶部１６のみにＩＰｓｅｃポリシーを設定すればよいため、誤ってそれぞれのＩＰｓｅｃ処理装置２ａ～２ｆに異なる設定をしてしまう事故を回避することができると同時に、ユーザが実際に入力する設定の数も減らすことができる。

【００５５】

図４は図２の管理テーブル１７の記憶内容を示す図である。図４において、管理テーブル１７にはＩＰｓｅｃ処理装置２ａ～２ｆから送られる要求メッセージに含まれる要求元アドレス、相手先アドレス、ＩＤ、ＳＰＩ（Ｓｅｃｕｒｉｔｙ Ｐａｒａｍｅｔｅｒ Ｉｎｄｅｘ：セキュリティパラメータインデックス）をそれぞれ記録する要求元アドレス欄、相手先アドレス欄、要求ＩＤ欄、ＳＰＩ欄と、当該通信用のＩＰｓｅｃ処理に必要となるパラメータ群を記録する設定パラメータ欄とがある。このうち、設定パラメータ欄には当該通信に適用するポリシー及び当該通信用ＳＡの構築に必要なパラメータからなるＳＡパラメータが設定される。

【００５６】

図５は図４のＳＡパラメータの内容を示す図である。図５において、ＳＡパラメータはＩＰｓｅｃプロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、有効期限、暗号鍵、認証鍵、ＩＶ（Ｉｎｉｔｉａｌｉｚａｔｉｏｎ Ｖｅｃｔｏｒ）と、当該通信の受信側ＩＰｓｅｃ処理装置２ａ～２ｆで使用するＳＰＩ値からなる。

【００５７】

１個のＩＰｓｅｃ通信に対して、通信を行う両端のＩＰｓｅｃ処理装置２ａ～２ｆから要求が発生するため、管理テーブル１７の１個のエントリには要求元アドレス、相手先アドレス、要求ＩＤ、ＳＰＩは２個ずつ存在する。また、同一のＩＰｓｅｃ通信であっても、ＳＡの有効期限満了に備えて新しいＳＡが要求される場合があり、この場合には管理テーブル１７には新しいＳＡのために新しく１個のエントリが登録される。尚、管理テーブル１７の内容はすべて要求処理部１５によって自動的に設定されるため、管理テーブル１７の内容をユーザが直接設定する必要はない。

【００５８】

管理テーブル１７を参照することで、ＩＰｓｅｃ処理装置２ａ～２ｆに配布する設定パラメータを得ることができる。設定パラメータ内のＳＡパラメータはＩＰｓｅｃ通信を実施するそれぞれのＩＰｓｅｃ処理装置２ａ～２ｆからの要求メッセージを受信することで確定するため、片方のＩＰｓｅｃ処理装置２ａ～２ｆからしか要求メッセージを受信していない場合には、相手側の要求ＩＤ欄及びＳＰＩ欄が空欄となり、設定パラメータ欄のＳＡパラメータも空欄となる。但し、適用ポリシーについては片方のＩＰｓｅｃ処理装置２ａ～２ｆから要求メッセージを受信するだけで確定するため、片方のＩＰｓｅｃ処理装置２ａ～２ｆから要求メッセージを受信するだけで、適用するポリシーが設定される。

【００５９】

図４に示す例では、１番目のエントリにＩＰｓｅｃ処理装置２ａとＩＰｓｅｃ処理装置２ｂとの通信に適用されるポリシー及びＳＡパラメータがそれぞれ登録されている。２番目のエントリには同じくＩＰｓｅｃ処理装置２ａとＩＰｓｅｃ処理装置２ｂとの通信に適用されるポリシーが登録されているが、ＩＰｓｅｃ処理装置２ｂから対応する設定要求メッセージを受信していないためＳＡパラメータが確定していない。

【００６０】

図５に図４内のＳＡパラメータ（ａ）の内容を示す。ＳＡパラメータは配布ポリシーの内容、設定要求メッセージで通知されたＳＰＩ、及び乱数生成器１８から得られる乱数を基に要求処理部１５によって生成される。

【００６１】

要求処理部１５はＩＰｓｅｃ処理装置２ａ～２ｆから要求メッセージを受信して、ＩＰｓｅｃ処理装置２ａ～２ｆに要求起動メッセージや配布メッセージ、エラーメッセージを送信する。

【００６２】

図６は本発明の一実施例による要求メッセージの一例を示す図である。図６において、要求メッセージには要求メッセージを他の要求メッセージと区別するためのＩＤ「１００１」と、要求メッセージを送信したＩＰｓｅｃ処理装置２ａ～２ｆのアドレスを示す要求元アドレス「ＩＰｓｅｃ処理装置２ａ」と、相手とな

るＩＰｓｅｃ処理装置２ａ～２ｆのアドレスを示す相手先アドレス「ＩＰｓｅｃ処理装置２ｂ」と、要求元で使用するＳＰＩの値「５１００」とが含まれている。

【００６３】

尚、本実施例では２台のＩＰｓｅｃ処理装置２ａ～２ｆ間に存在するＩＰｓｅｃ通信を１種類に限定しているため、両方のＩＰｓｅｃ処理装置２ａ～２ｆのアドレスが決まれば、適用するＩＰｓｅｃポリシーを一意に特定することができる。したがって、要求メッセージにはＩＰｓｅｃ通信の両端のアドレスを設定している。これ以外に、２台のＩＰｓｅｃ処理装置２ａ～２ｆ間に複数のＩＰｓｅｃ通信を設定したい場合が考えられる。そのような場合には、それぞれのＩＰｓｅｃ通信を特定するために必要な情報（例えば、プロトコル番号やポート番号等）を要求メッセージに設定する。

【００６４】

図７は本発明の一実施例による配布メッセージの一例を示す図であり、図８は本発明の一実施例による要求起動メッセージの一例を示す図であり、図９は本発明の一実施例による該当なしエラーメッセージの一例を示す図であり、図１０は本発明の一実施例による内容不一致エラーメッセージの一例を示す図であり、図１１は本発明の一実施例による応答なしエラーメッセージの一例を示す図である。

【００６５】

図１２及び図１３は本発明の一実施例によるＩＰｓｅｃ設定サーバ１の動作を示すフローチャートである。これら図１～図１３を参照して本発明の一実施例によるＩＰｓｅｃ設定サーバ１の動作について説明する。まず、要求処理部１５が要求メッセージを受信した場合の動作について説明する。

【００６６】

要求処理部１５はＩＰｓｅｃ処理装置２ａ～２ｆから要求メッセージを受信すると　（図１２ステップＳ１）、管理テーブル１７の中から要求メッセージに含まれる要求元アドレス、相手先アドレス、ＩＤが一致するエントリを検索する（図１２ステップＳ２）。

【００６７】

要求処理部１５は一致するエントリが見つかると、一致したエントリのＳＰＩが要求メッセージに含まれるＳＰＩと一致するかどうかを確認する（図１２ステップＳ３）。要求処理部１５はＳＰＩが一致しなければ、ＩＰｓｅｃ処理装置２ａ～２ｆに内容不一致エラーメッセージを送信する（図１２ステップＳ８）。

【００６８】

この時、内容不一致エラーメッセージには要求メッセージに含まれるＩＤ、要求元アドレス、相手先アドレスと、エントリ一覧とを設定する。エントリ一覧には管理テーブル１７に含まれるエントリの中で、要求元アドレスと相手先アドレスとが一致するすべてのエントリを設定する。但し、エントリ一覧に設定する項目は各エントリの要求ＩＤとそのエントリで使用される要求元アドレス用のＳＰＩだけである。

【００６９】

ＩＰｓｅｃ処理装置２ａ～２ｆは内容不一致エラーメッセージを受信することでＩＰｓｅｃ設定サーバ１が管理している設定情報と、ＩＰｓｅｃ処理装置２ａ～２ｆが把握している設定情報との差分を知ることができる。

【００７０】

この内容不一致エラーメッセージの一例を図１０に示す。図１０において、ＩＰｓｅｃ設定サーバ１上においてＩＰｓｅｃ処理装置２ａとＩＰｓｅｃ処理装置２ｂとの通信用にすでに「１００１」，「１００２」という要求ＩＤによって設定情報が生成されており、そこで使用しているＳＰＩの値がそれぞれ「５１００」，「５１１０」であることがわかる。

【００７１】

要求処理部１５は管理テーブル１７の中に要求メッセージに含まれる要求元アドレス、相手先アドレス、ＩＤと一致するエントリが見つかってＳＰＩの内容も一致した場合、管理テーブル１７内の当該エントリの相手側の要求ＩＤ欄を確認する（図１２ステップＳ４）。

【００７２】

要求処理部１５は相手側の要求ＩＤ欄が設定されている場合、すでに管理テー

ブル１７の設定パラメータ欄が確定しているため、要求メッセージの送信元に配布メッセージを送信する（図１２ステップＳ５）。配布メッセージには要求メッセージに含まれる要求元アドレス、送信元アドレス、ＩＤを設定し、設定パラメータには管理テーブル１７内の配布ポリシーとＳＡパラメータとを設定する。この場合は、すでに返送すべき設定パラメータがすべて確定している場合である。

【００７３】

この配布メッセージの一例を図７に示す。図７に示す例では、設定パラメータには配布ポリシー（ａ）とＳＡパラメータ（ａ），ＳＡパラメータ（ｂ）が設定されている。ＩＰｓｅｃ処理装置２ａは配布ポリシー（ａ）とＳＡパラメータ（ａ），ＳＡパラメータ（ｂ）とを使用して双方向のＩＰｓｅｃ通信を実施することができる。

【００７４】

要求処理部１５は管理テーブル１７の中に要求メッセージに含まれる要求元アドレス、相手先アドレス、ＩＤと一致するエントリが見つかってＳＰＩの内容も一致した場合で、相手側の要求ＩＤ欄が設定されていなかった場合、そのまま処理を終了する（図１２ステップＳ６）。この場合には、すでにＩＰｓｅｃ処理装置２ａ～２ｆから同一の要求メッセージを受信しているが、相手側の情報がないため、相手側の情報を待っている状態である。

【００７５】

要求処理部１５は管理テーブル１７の中に要求元アドレス、相手先アドレス、ＩＤが一致するエントリがなかった場合、要求メッセージに含まれる要求元アドレス、相手先アドレス、ＳＰＩをキーにして管理テーブル１７を検索する（図１２ステップＳ７）。

【００７６】

要求処理部１５は一致するエントリが見つかると、要求メッセージの送信元に内容不一致エラーメッセージを送信して処理を終了する（図１２ステップＳ８）。これは既にＩＰｓｅｃ設定サーバ１に登録済みのＳＰＩを重複して使用してＩＰｓｅｃ処理装置２ａ～２ｆが新しい設定パラメータを要求した場合である。ＩＰｓｅｃ処理装置２ａ～２ｆは内容不一致エラーメッセージを受信することで、

ＳＰＩの重複を検出し、重複しないＳＰＩを選択することができる。

【００７７】

要求処理部１５は管理テーブル１７の中に要求元アドレス、相手先アドレス、ＩＤが一致するエントリがなく、ＳＰＩの重複も検出されなければ、要求メッセージに含まれる要求元アドレスと相手先アドレスとをキーにして管理テーブル１７を検索する（図１２ステップＳ９）。この時、要求処理部１５は要求ＩＤ欄が空欄のエントリを検索する。

【００７８】

一致するエントリが存在した場合には、すでに相手側のＩＰｓｅｃ処理装置２ａ～２ｆから当該通信に対する要求メッセージが送信されており、設定パラメータの適用ポリシーまで確定している状態である。要求処理部１５は空欄になっている要求ＩＤ欄及びＳＰＩ欄に要求メッセージに設定されているＩＤ及びＳＰＩを設定し、設定パラメータ欄の適用ポリシーで示されるポリシーにしたがって、それぞれの方向用にＳＡパラメータを生成する。

【００７９】

具体的に述べると、ＩＰｓｅｃプロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、有効期限については適用ポリシーと同一の内容を設定し、暗号化鍵、認証鍵、ＩＶについては乱数生成器１８から乱数を取得して値を決定し、受信側ＳＰＩ欄には受信側のＩＰｓｅｃ処理装置２ａ～２ｆが使用するＳＰＩの値を設定する。

【００８０】

要求処理部１５はそれぞれの方向用のＳＡパラメータが生成できたら、管理テーブル１７の設定パラメータ欄に登録する（図１２ステップＳ１０）。要求処理部１５は管理テーブル１７にＳＡパラメータを登録すると、要求メッセージの送信元であるＩＰｓｅｃ処理装置２ａ～２ｆの要求ＩＤと、設定パラメータを設定した配布メッセージをＩＰｓｅｃ処理装置２ａ～２ｆに送信すると同時に、相手先となるＩＰｓｅｃ処理装置２ａ～２ｆに対しても、相手先の要求ＩＤを含む配布メッセージを送信する（図１２ステップＳ１１）。

【００８１】

また、要求処理部１５はタイマ１９を使用してＳＡパラメータの有効期限と同じ時間を計測し、タイマ１９が満了した時点で、管理テーブル１７の当該エントリを削除する。

【００８２】

要求処理部１５は管理テーブル１７の中に要求元アドレスと要求ＩＤとが一致するエントリがなく、要求元アドレスと相手先アドレスとをキーとした検索でも一致するエントリがなかった場合、要求メッセージに含まれる要求元アドレスと相手先アドレスとの組をキーにして配布ポリシー記憶部１６を検索する（図１３ステップＳ２１）。

【００８３】

要求処理部１５は該当するエントリが見つからなければ、ＩＰｓｅｃ処理装置２ａ～２ｆに該当なしエラーメッセージを送信する（図１３ステップＳ２６）。該当なしエラーメッセージには要求メッセージに含まれていたＩＤ、要求元アドレス、相手先アドレスを設定する。この該当なしエラーメッセージの一例を図９に示す。

【００８４】

要求処理部１５は配布ポリシー記憶部１６内に一致するエントリが存在した場合、管理テーブル１７の新しいエントリの要求元アドレス、相手先アドレス、要求ＩＤ、ＳＰＩ欄にそれぞれ要求メッセージに含まれる要求元アドレス、相手先アドレス、ＩＤ、ＳＰＩを設定する。同一エントリのもう一つの要求元アドレスには要求メッセージの相手先アドレスを、相手先アドレスには要求メッセージの要求元アドレスを設定し、要求ＩＤ、ＳＰＩは空欄とする。

【００８５】

また、要求処理部１５は配布ポリシー記憶部１６の該当エントリに含まれる配布ポリシーを管理テーブル１７の設定パラメータ欄に設定する（図１３ステップＳ２２）。この時点で、ＳＡパラメータを生成するために必要なパラメータ群のうち、暗号化鍵、認証鍵等の共有秘密鍵、相手先ＩＰｓｅｃ処理装置２ａ～２ｆで使用するＳＰＩ以外のパラメータがすべて確定する。共有秘密鍵は乱数生成器１９から得られる乱数を使用するため、相手先のＳＰＩさえ確定すれば、ＳＡパ

ラメータを生成することが可能となる。

【００８６】

要求処理部１５は配布ポリシー記憶部１６内に一致するエントリが存在し、管理テーブル１７に要求元のＩＰｓｅｃ処理装置２ａ～２ｆからの要求に応じてエントリを登録した後、相手先のＩＰｓｅｃ処理装置２ａ～２ｆに対して要求起動メッセージを送信する（図１３ステップＳ２３）。要求起動メッセージには要求メッセージの要求元アドレスを設定する。この要求起動メッセージの一例を図８に示す。

【００８７】

要求処理部１５は要求起動メッセージを送信すると、５秒間隔で要求起動メッセージの送信を繰り返し、要求起動メッセージの送信先のＩＰｓｅｃ処理装置２ａ～２ｆから管理テーブル１７の該当エントリに対応する要求メッセージを受信するか、要求起動メッセージを６回送信すると、要求起動メッセージの送信を停止する。繰り返し送信することによって、１個の要求起動メッセージが紛失した場合にも他の要求起動メッセージによって処理を継続することができる。

【００８８】

要求処理部１５は６回の要求起動メッセージ送信によって送信を停止した場合（図１３ステップＳ２４）、管理テーブル１７から該当エントリを削除し（図１３ステップＳ２７）、要求メッセージの送信元のＩＰｓｅｃ処理装置２ａ～２ｆには応答なしエラーメッセージを送信する（図１３ステップＳ２８）。応答なしエラーメッセージには、ＩＰｓｅｃ処理装置２ａ～２ｆからの要求メッセージに含まれていたＩＤ、要求元アドレス、相手先アドレスを設定する。この応答なしエラーメッセージの一例を図１１に示す。

【００８９】

要求処理部１５は要求起動メッセージに対して、管理テーブル１７の該当エントリに対応する要求メッセージを受信した場合（図１３ステップＳ２４）、要求起動メッセージの送信を停止し、要求メッセージ受信時の動作を行う（図１３ステップＳ２５）。

【００９０】

タイマ１９は要求処理部１５に依頼されて時間を計測し、指定された時間が経過したら要求処理部１５に通知する。タイマ１９は同時に複数の時間を計測することができる。

【００９１】

上記のように、要求起動メッセージを送信しているので、要求メッセージの送信元のＩＰｓｅｃ処理装置に対向するＩＰｓｅｃ処理装置ではその送信元のＩＰｓｅｃ処理装置でのＩＰｓｅｃのポリシーの設定とほぼ同時にＩＰｓｅｃのポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元のＩＰｓｅｃ処理装置がパケットを暗号化して送信すると、対向するＩＰｓｅｃ処理装置では送信元のＩＰｓｅｃ処理装置からのパケットを復号して受取ることができる。よって、ポリシー設定後の暗号化や復号を滞りなく行うことができる。

【００９２】

この場合、パケットの復号ができなくてそのパケットを破棄したり、パケットの復号を誤って行ったりすることがないので、送信先のＩＰｓｅｃ処理装置において送信元からのパケットを取りこぼしなく受取ることができる。

【００９３】

また、要求起動メッセージの送信時にそれに応答した要求メッセージを対向するＩＰｓｅｃ処理装置から受信しなければ、送信元のＩＰｓｅｃ処理装置に対して応答なしエラーメッセージを送信するので、送信元のＩＰｓｅｃ処理装置では対向装置の不存在を即座に認識することができる。

【００９４】

図１４は図１のＩＰｓｅｃ処理装置２ａ～２ｆの構成を示すブロック図である。図１４においてはＩＰｓｅｃ処理装置２ａ～２ｆをまとめてＩＰｓｅｃ処理装置２としており、ＩＰｓｅｃ処理装置２ａ～２ｆはＩＰｓｅｃ処理装置２と同様の構成である。

【００９５】

ＩＰｓｅｃ処理装置２は主にコンピュータから構成され、ＩＰｓｅｃ設定サーバ１を利用する。つまり、ＩＰｓｅｃ処理装置２はインタフェース部（Ｉ／Ｆ）２１，２２と、ＩＰｓｅｃ処理部２３と、ＳＰＤ２４と、ＳＡＤ２５と、設定管

理部２６と、ルーティング部２７と、記録媒体２８とを具備し、上記の各部の動作はコンピュータが記録媒体２８のプログラムを実行することで実現される。

【００９６】

インタフェース部２１はプライベートネットワーク２００（図１のプライベートネットワーク２０１～２０４）に接続され、プライベートネットワーク２００とのデータ通信を行う。インタフェース部２２はインタネット１００に接続され、インタネット１００を介したデータ通信を行う。

【００９７】

ＩＰｓｅｃ処理部２３はインタフェース部２１，２２から受信したデータ通信パケットに対してＩＰｓｅｃ処理を実施する。設定管理部２６はＩＰｓｅｃ処理部２３に依頼され、必要な設定をＩＰｓｅｃ設定サーバ１に要求する。

【００９８】

ＳＰＤ２４はＩＰｓｅｃ処理部２３及び設定管理部２６から参照され、ＩＰｓｅｃを適用するためのポリシーを記録している。ＳＡＤ２５はＩＰｓｅｃ処理部２３と設定管理部２６とから参照され、個々の通信に対してＩＰｓｅｃ処理を実施するために必要なＳＡを記録している。ルーティング部２７はＩＰｓｅｃ処理部２３と設定管理部２６との間でデータ通信パケットの送受信を行い、各々のデータ通信パケットの転送先を決定する。

【００９９】

ＩＰｓｅｃ処理装置２の構成は図３１に示す従来のＩＰｓｅｃ処理装置の構成と比較すると、ＩＰｓｅｃ処理装置２では設定管理部２６が追加されている点が異なる。また、後述するように、ＳＰＤ２４に新しい項目がされた点と、ＩＰｓｅｃ処理部２３に新しい動作が加えられた点とが異なる。

【０１００】

インタフェース部２１はプライベートネットワーク２００からデータ通信パケットを受信してＩＰｓｅｃ処理部２３に転送し、またＩＰｓｅｃ処理部２３から転送されたデータ通信パケットをプライベートネットワーク２００に送信する。

【０１０１】

インタフェース部２２はインタネット１００からデータ通信パケットを受信し

てＩＰｓｅｃ処理部２３に転送し、またＩＰｓｅｃ処理部２３から転送されたデータ通信パケットをインタネット１００に送信する。

【０１０２】

ＳＰＤ２４には個々のＳＰＤエントリを識別し、優先順位を明確にするためのＩＤ欄と、トラヒックを選択するためのセレクタ欄、選択されたトラヒックに対する処理欄、ＩＰｓｅｃ処理を適用する場合のＩＰｓｅｃのパラメータ情報等を記録するＩＰｓｅｃ適用ポリシー欄、及びＳＰＤ検索時にＩＰｓｅｃ設定サーバ１に設定を要求するか否かを判断するための設定要求用相手アドレス欄が存在する。

【０１０３】

図１５は図１４のＳＰＤ２４の内容を示す図である。図１５において、ＳＰＤ２４は設定要求用相手アドレス欄が追加されている以外は通常のＩＰｓｅｃで用いられるＳＰＤと同一のものである。尚、ＳＰＤ２４は送信用と受信用とが存在する。

【０１０４】

ＳＰＤ２４はＩＰｓｅｃ処理部２３がデータ通信パケットを受信した場合に、そのパケットの扱いを決定するために用いられる。ＩＰｓｅｃ処理部２３はＩＰｓｅｃが適用されていないデータ通信パケットを受信すると、ＳＰＤ２４のセレクタ欄と比較して一致するエントリを探す。一致するエントリが発見されると、処理欄にしたがって当該パケットの扱いを決定する。

【０１０５】

処理欄には“ＩＰｓｅｃ適用”，“通過”，“廃棄”のいずれかが格納される。特に、“ＩＰｓｅｃ適用”の処理となった場合には、ＩＰｓｅｃポリシー欄の内容にしたがって引き続きＩＰｓｅｃの処理が行われる。

【０１０６】

本実施例ではＳＰＤ２４に存在する設定要求用相手アドレス欄において、処理欄が“ＩＰｓｅｃ適用”となった場合にそのＩＰｓｅｃ適用ポリシー欄をＩＰｓｅｃ設定サーバ１に要求するか否かを判断するために使用すると同時に、ＩＰｓｅｃ設定サーバ１に設定を要求する場合に、要求する設定パラメータを特定する

ための識別子としても使用する。

【０１０７】

尚、ＳＰＤ２４の内容は標準のＩＰｓｅｃと同様に、基本的に予めすべて設定しておく必要があるが、設定要求用相手アドレスを設定したエントリについてはＩＰｓｅｃ適用ポリシーを省略することが可能である。この場合には設定管理部２６がＩＰｓｅｃ設定サーバ１から必要なＩＰｓｅｃ適用ポリシー情報を入手し、自動的にＳＰＤ２４のＩＰｓｅｃ適用ポリシー欄を設定する。この時、ＩＰｓｅｃ設定サーバ１との通信を暗号化するための設定だけは適用ポリシーを省略することはできない。

【０１０８】

図１５に示す例では、ＩＰｓｅｃ処理装置２ａ自身からＩＰｓｅｃ設定サーバ１宛のパケットに対して適用ポリシー（ｚ）にしたがってＩＰｓｅｃ処理を実施し、プライベートネットワーク２０２宛のパケット、及びプライベートネットワーク２０３宛のパケットに対してＩＰｓｅｃ処理を適用するが、そのポリシーはＩＰｓｅｃ設定サーバ１から取得し、それ以外のすべてのパケットはＩＰｓｅｃ処理を適用せずに通過させる設定となっている。

【０１０９】

図１６は図１５に示すＳＰＤ２４の適用ポリシー（ｚ）の一例を示す図である。図１６において、ＩＰｓｅｃ適用ポリシーにはＩＰｓｅｃ通信で使用するプロトコルやカプセル化モード、暗号化アルゴリズム、認証アルゴリズム等、適用するＩＰｓｅｃ処理を特定するために必要な情報が設定される。

【０１１０】

図１６に示す例では、暗号化アルゴリズムに「ＡＥＳ－ＣＢＣ」、認証アルゴリズムに「ＨＭＡＣ－ＳＨＡ－１－９６」を使用してＥＳＰの「トランスポートモード」を適用することと、ＳＡの有効期間が「３６００秒」であることが示されている。尚、使用するプロトコルや暗号化アルゴリズム等によって必要となるパラメータが異なるため、それぞれの適用ポリシーにおいては図１６に示すパラメータ以外のパラメータが現れる場合や、図１６の中の一部のパラメータが存在しない場合もある。

【０１１１】

従来のＩＰｓｅｃでは適用ポリシーをＩＰｓｅｃ処理装置に予めすべてユーザが設定しておく必要があるが、前項で述べた通り、本実施例のＳＰＤ２４では適用ポリシーの設定を省略することが可能である。その場合には設定管理部２６によってＩＰｓｅｃ設定サーバ１から取得したＩＰｓｅｃ適用ポリシーが自動的に設定される。

【０１１２】

尚、ＩＫＥを使用する場合にはＩＫＥ自身に必要となるパラメータがＳＰＤ２４のＩＰｓｅｃ適用ポリシーとは独立して存在する。しかしながら、本実施例の観点から見ると、ＩＰｓｅｃ通信を行うために、本来ユーザが設定しなければならないパラメータであって、本実施例のＩＰｓｅｃ設定サーバ１を使用することによって省略可能なパラメータである、という点においてＩＰｓｅｃ適用ポリシーと同等である。そこで、説明を容易にするため、ＳＰＤ２４のＩＰｓｅｃ適用ポリシーがＩＫＥを使用するポリシーの場合には、そのポリシーの中にＩＫＥ用のパラメータもすべて含まれているものとして扱う。そのため、図１６に示す例ではＩＫＥ用の設定パラメータも含まれている。実際の構成においては依然としてＩＫＥ自身の設定はＩＰｓｅｃ適用ポリシーとは独立である。

【０１１３】

図１７は図１４のＳＡＤ２５の内容を示す図である。図１７において、ＳＡＤ２５には個々のＩＰｓｅｃ通信に必要となるＳＡが登録される。すなわち、ＳＡＤ２５はＳＡを管理するためのデータベースである。

【０１１４】

ＳＰＤ２４のＩＰｓｅｃ適用ポリシーでは、適用するＩＰｓｅｃ処理（どのような種類のＩＰｓｅｃ処理を施すか）を示すための情報が示されるが、実際にＩＰｓｅｃ処理を行うためには追加の情報が必要となる。

【０１１５】

例えば、ＩＫＥを使用する場合には、ＩＰｓｅｃ処理で使用する暗号化鍵や認証鍵を相手ＩＰｓｅｃ処理装置と交換し、それらの値を使用することで初めて一つのＩＰｓｅｃ処理が実施することができる。このように、一つのＩＰｓｅｃ処

理を実施するために必要なパラメータ群をＳＡと呼ぶ。

【０１１６】

ＳＡＤ２５には個々のＳＡＤエントリを識別するためのＩＤと、ＩＰｓｅｃ通信の相手アドレスを示す終点アドレスと、ＩＰｓｅｃ通信で使用されるＩＰｓｅｃプロトコルと、個々のＳＡに固有の識別子であるＳＰＩ及びその他のＳＡパラメータとによって構成される。

【０１１７】

ＳＡＤ２５は設定管理部２６あるいはＩＰｓｅｃ処理部２３によって自動的に設定されるため、ＳＡＤ２５をユーザが直接設定する必要はない。尚、ＳＡＤ２５は標準のＩＰｓｅｃで用いられるＳＡＤと同一のものであり、送信用と受信用とが存在する。

【０１１８】

図１７に示す例では、１番目のエントリにＩＰｓｅｃ処理装置２ａとＩＰｓｅｃ処理装置２ｂとの間のＳＡが、２番目のエントリにＩＰｓｅｃ処理装置２ａとＩＰｓｅｃ設定サーバ１との間のＳＡが登録されている。

【０１１９】

図１８は図１４のＩＰｓｅｃ処理部２３の処理動作を示すフローチャートであり、図１９及び図２０は図１４の設定管理部２６の処理動作を示すフローチャートである。これら図１８～図２０を参照してＩＰｓｅｃ処理装置２ａ～２ｆの動作について説明する。

【０１２０】

ＩＰｓｅｃ処理部２３はプライベートネットワーク２００からインタネット１００宛のデータ通信パケットを受信すると（図１８ステップＳ３１）、データ通信パケットとＳＰＤ２４のセレクタ欄とを比較して該当するエントリを検索する（図１８ステップＳ３２）。該当するエントリの設定要求用相手アドレス欄が空欄の場合には、従来のＩＰｓｅｃと同一の動作である（図１８ステップＳ３３）。

【０１２１】

尚、この従来のＩＰｓｅｃの動作によって、ＩＰｓｅｃ処理装置２とＩＰｓｅ

ｃ設定サーバ１とのメッセージの送受信は保護される。すなわち、予め通常のＩＰｓｅｃの方法に従ってＩＰｓｅｃ処理装置２とＩＰｓｅｃ設定サーバ１との間の通信についてはＳＰＤ２４に登録しておく。

【０１２２】

ＩＰｓｅｃ処理部２３はＳＰＤ２４の検索で該当するエントリの設定要求用相手アドレス欄が設定されていた場合で、ＩＰｓｅｃ適用ポリシー欄が設定されている場合、さらにＳＡＤ２５から当該通信用のＳＡを検索する（図１８ステップＳ３４）。当該通信用のＳＡが存在する場合には、従来のＩＰｓｅｃと同一の動作となり、ＳＡの内容にしたがってデータ通信パケットにＩＰｓｅｃ処理を適用する（図１８ステップＳ３３）。

【０１２３】

ＩＰｓｅｃ処理部２３はＳＰＤ２４の検索で該当するエントリの設定要求用相手アドレス欄が設定されており、ＩＰｓｅｃ適用ポリシー欄も設定されている場合で、ＳＡＤ２５に該当エントリがない場合、あるいはそもそもＩＰｓｅｃ適用ポリシー欄が設定されていない場合、当該データ通信パケットの処理を一時中断し、設定管理部２６に設定サーバから設定を取得するように依頼する（図１８ステップＳ３５）。この時、設定管理部２６にはＳＰＤ２４の当該エントリのＩＤを通知する。

【０１２４】

ＩＰｓｅｃ処理部２３は設定管理部２６に依頼した後、設定管理部２６から結果が通知されるまで同一のＳＰＤエントリに対する依頼は行わない。ＩＰｓｅｃ処理部２３は設定管理部２６から設定完了の通知を受けると（図１８ステップＳ３６）、データ通信パケットのＩＰｓｅｃ処理を再開する（図１８ステップＳ３３）。この時点では、必要なポリシー及びＳＡが設定管理部２６によって設定されており、従来通りのＩＰｓｅｃ処理を実施するのみとなる。

【０１２５】

ＩＰｓｅｃ処理部２３は設定管理部２６から設定失敗の通知を受けると（図１８ステップＳ３３）、一時中断していたデータ通信パケット処理を中止する（図１８ステップＳ３７）。

【０１２６】

ＩＰｓｅｃ処理部２３はインタネット１００からプライベートネットワーク２００宛のＩＰｓｅｃ適用済みデータ通信パケットを受信した場合、従来のＩＰｓｅｃと同様に動作する。すなわち、ＩＰｓｅｃ処理部２３はＳＡＤ２４から該当するエントリを検索し、一致するエントリが存在した場合、その内容にしたがってＩＰｓｅｃの復号処理を実施する。ＩＰｓｅｃ処理部２３は一致するエントリが存在しない場合、そのデータ通信パケットを廃棄する。

【０１２７】

ＩＰｓｅｃ処理部２３は従来のＩＰｓｅｃと同様に、ＳＡＤ２５内の各ＳＡエントリの有効期限を確認し、有効期限が満了する前に新しいＳＡの確立を行う。この時、当該ＳＡがＩＰｓｅｃ設定サーバ１によって生成されたＳＡだった場合、ＩＰｓｅｃ処理部２３は設定管理部２６にＩＰｓｅｃ設定サーバ１から設定を取得するように依頼する。

【０１２８】

設定の取得を依頼する時、ＩＰｓｅｃ処理部２３は設定管理部２６に当該ＳＡに対応するＳＰＤ２４エントリのＩＤを通知する。設定管理部２６からは依頼に対する結果が通知されるが、ＩＰｓｅｃ処理部２３はその結果の通知を無視する。

【０１２９】

設定管理部２６はＩＰｓｅｃ処理部２３から設定取得の依頼を受けると（図１９ステップＳ４１）、通知されたＳＰＤ２４のエントリ用の要求メッセージを生成する（図１９ステップＳ４２）。要求メッセージにはＩＤと、要求元アドレスと、相手先アドレスと、要求元で使用するＳＰＩの値とを設定する。ＩＤには他の要求メッセージと重複しない任意の数値を設定し、ＳＰＩにはＩＰｓｅｃ通信において自己が使用するつもりのＳＰＩを設定する。要求元アドレスにはＩＰｓｅｃ処理装置２のアドレスを設定する。相手先アドレスには、当該ＳＰＤ２４のエントリに含まれる設定要求用相手アドレスを設定する。

【０１３０】

ＩＰｓｅｃ設定サーバ１からの応答メッセージには設定管理部２６が送信した

メッセージのＩＤと要求元アドレス、相手先アドレスが含まれるため、設定管理部２６はどのメッセージに対する応答なのかを識別することができる。

【０１３１】

この要求メッセージの一例を図６に示す。図６に示す例はＩＰｓｅｃ処理装置２ａがＩＰｓｅｃ処理装置２ｂとのＩＰｓｅｃ通信に必要な設定を要求する要求メッセージの例である。

【０１３２】

設定管理部２６は生成した要求メッセージをＩＰｓｅｃ設定サーバ１に送信する（図１９ステップＳ４３）。設定管理部２６はＩＰｓｅｃ設定サーバ１に要求メッセージを送信すると、５秒間隔で要求メッセージの送信を繰り返し、ＩＰｓｅｃ設定サーバ１から要求メッセージに対応する応答を受信するか、要求メッセージを６回送信すると、要求メッセージの送信を停止する。

【０１３３】

設定管理部２６は６回の要求メッセージ送信によって送信を停止した場合や、該当なしエラーメッセージあるいは応答なしエラーメッセージを受信した場合（図１９ステップＳ４４，Ｓ４７）、ＩＰｓｅｃ処理部２３に設定失敗を通知して処理を終了する（図１９ステップＳ４９）。

【０１３４】

尚、設定管理部２６は要求メッセージの送信を繰り返す場合、常に同じＩＤ、同じＳＰＩを使用して送信する。繰り返し送信することによって、１個の要求メッセージが紛失した場合にも他の要求メッセージによって処理を継続することができる。

【０１３５】

設定管理部２６はＩＰｓｅｃ設定サーバ１から内容不一致エラーメッセージを受信した場合（図１９ステップＳ４７）、内容不一致エラーメッセージに含まれるエントリ一覧を確認し、エントリ一覧に含まれるＩＤ及びＳＰＩ以外の値を用いて改めてＩＤとＳＰＩとを選択し、要求メッセージをＩＰｓｅｃ設定サーバ１に送信する（図１９ステップＳ４８）。

【０１３６】

これはＩＰｓｅｃ処理装置２が何らかの原因で動作情報を喪失した後、既にＩＰｓｅｃ設定サーバ１側に登録済みのＩＤあるいはＳＰＩを使用して要求メッセージを送信した場合である。

【０１３７】

設定管理部２６は内容不一致エラーメッセージで通知されたＩＤやＳＰＩ以外の値を使用することで、ＩＰｓｅｃ設定サーバ１の既存の情報と矛盾しない新しい要求メッセージを生成することができる。

【０１３８】

設定管理部２６はＩＰｓｅｃ設定サーバ１から配布メッセージを受信した場合（図１９ステップＳ４４）、配布メッセージに含まれる適用ポリシーを当該ＳＰＤ２４のＩＰｓｅｃ適用ポリシー欄に設定し、配布メッセージに含まれるＳＡパラメータを使用してＳＡを生成し、ＳＡＤ２５に登録する（図１９ステップＳ４５）。設定管理部２６はＳＡをＳＡＤ２５に登録したら、ＩＰｓｅｃ処理部２３に設定完了を通知し、処理を終了する（図１９ステップＳ４６）。

【０１３９】

設定管理部２６はＩＰｓｅｃ設定サーバ１から要求起動メッセージを受信した場合　（図２０ステップＳ５１）、ＳＰＤ２４のエントリの中から、設定要求用相手アドレスが要求起動メッセージに含まれる相手先アドレスと一致するエントリを検索する（図２０ステップＳ５２）。一致するエントリが見つからない場合、設定管理部２６は要求起動メッセージを無視する（図２０ステップＳ５３）。

【０１４０】

この場合、ＩＰｓｅｃ設定サーバ１からは６回要求起動メッセージが送信されるが、その後、ＩＰｓｅｃ設定サーバ１は要求起動メッセージの送信を停止し、元々要求メッセージを送信したＩＰｓｅｃ処理装置２にはＩＰｓｅｃ設定サーバ１からエラーメッセージが送信される。

【０１４１】

設定管理部２６はＳＰＤ２４の検索によって一致するエントリを見つけた場合、ＩＰｓｅｃ処理部２３からＳＰＤ２４のエントリに対する設定取得依頼を受信した時と同様に動作する。すなわち、設定管理部２６は要求メッセージを生成し

てＩＰｓｅｃ設定サーバ１に最大６回繰り返し送信する（図２０ステップＳ５４，Ｓ５５）。

【０１４２】

但し、ＩＰｓｅｃ処理部２３の依頼による送信ではないので、ＩＰｓｅｃ設定サーバ１から配布メッセージやエラーメッセージを受信しても、ＩＰｓｅｃ処理部２３にはその結果を通知しない（図２０ステップＳ５６，Ｓ５８，Ｓ６０）。

【０１４３】

また、設定管理部２３は要求起動メッセージに対して要求メッセージの送信を開始した場合、繰り返し送信が停止するまで、同一のＳＰＤ２４のエントリに対する要求起動メッセージを受信しても新たな要求メッセージの送信を行わない。

【０１４４】

一方、設定管理部２６はＩＰｓｅｃ設定サーバ１から配布メッセージを受信した場合（図２０ステップＳ５６）、配布メッセージに含まれる適用ポリシーを当該ＳＰＤ２４のＩＰｓｅｃ適用ポリシー欄に設定し、配布メッセージに含まれるＳＡパラメータを使用してＳＡを生成し、ＳＡＤ２５に登録する（図２０ステップＳ５７）。

【０１４５】

ルーティング部２７はＩＰｓｅｃ処理部２３からＩＰｓｅｃ復号処理済みのデータ通信パケットを受信して、当該パケットが設定管理部２６宛のパケットだった場合、当該パケットを設定管理部２６に転送する。当該パケットが設定管理部２６宛のパケットではない場合、ルーティング部２７は当該パケットを送信すべきインタフェースを決定し、再びＩＰｓｅｃ処理部２３を介して送信すべきインタフェースに転送する。

【０１４６】

また、ルーティング部２７は設定管理部２６からのデータ通信パケットを受信し、当該パケットを送信すべきインタフェースを決定して、ＩＰｓｅｃ処理部２３を介して転送する。

【０１４７】

図２１は図２のＳＰＤ１３の内容の一例を示す図であり、図２２は図２１に示

すＳＰＤ１３の適用ポリシー（ｖ）の内容を示す図であり、図２３は従来のＩＰｓｅｃ処理装置のＳＰＤの内容を示す図であり、図２４は図２３のＳＰＤの適用ポリシー（ｊ）の内容を示す図である。

【０１４８】

また、図２５は図２の管理テーブル１７のＩＰｓｅｃ処理装置２ａから要求メッセージを受信した後の内容を示す図であり、図２６は図１４のＳＰＤ２４の設定メッセージを受信して適用ポリシーを設定した後の内容を示す図であり、図２７は図２の管理テーブル１７のＳＡを更新するために新しいエントリが生成される場合の内容を示す図であり、図２８は本発明の一実施例によるＩＰｓｅｃ処理装置２の動作を示すシーケンスチャートである。

【０１４９】

これら図１～図２８を参照して本実施例のＩＰｓｅｃ設定サーバ１の具体的な動作について説明する。ここでは図１の中のＩＰｓｅｃ処理装置２ａに注目し、プライベートネットワーク２０１からプライベートネットワーク２０２宛のデータ通信に対してＩＰｓｅｃ処理装置２ａがＩＰｓｅｃ処理を実施する場合について説明する。まず、ＩＰｓｅｃ設定サーバ１、ＩＰｓｅｃ処理装置２ａ、ＩＰｓｅｃ処理装置２ｂに予め必要な設定項目について説明する。

【０１５０】

ＩＰｓｅｃ設定サーバ１にはＩＰｓｅｃ処理装置２ａ及びＩＰｓｅｃ処理装置２ｂとの間にそれぞれ安全なＩＰｓｅｃの経路を確保するために、従来と同様の方法で、ＳＰＤ１３を設定する。図２１に示すように、ＳＰＤ１３にはＩＰｓｅｃ設定サーバ１自身からＩＰｓｅｃ処理装置２ａ、ＩＰｓｅｃ処理装置２ｂ宛の通信に対して、それぞれ適用ポリシー（ｖ）、適用ポリシー（ｗ）にしたがってＩＰｓｅｃを適用するように設定している。

【０１５１】

この適用ポリシー（ｖ）の内容を図２２に示す。適用ポリシー（ｖ）にはＩＰｓｅｃ処理装置２ａとの通信を暗号化するためのポリシーが設定されている。また、ＩＰｓｅｃ処理装置２ａとの間のＩＰｓｅｃ通信においてＩＫＥによる鍵交換を実施するために、ＩＫＥに関するパラメータも設定しておく。

【０１５２】

尚、本来、ＩＫＥに関する設定はＩＰｓｅｃ適用ポリシーとは独立に存在するものであるが、説明を容易にするために、本実施例の説明においては適用ポリシーの一部として扱う。適用ポリシー（ｗ）の内容も適用ポリシー（ｖ）と同様の内容である。

【０１５３】

これらの設定によって、ＩＰｓｅｃ設定サーバ１とＩＰｓｅｃ処理装置２ａとの間に安全なＩＰｓｅｃの経路が設定され、設定情報及び秘密鍵の配布を安全に行うことができる。

【０１５４】

ＳＰＤ１３にはＩＰｓｅｃ設定サーバ１と通信するすべてのＩＰｓｅｃ処理装置２に対して１件ずつ設定を行う必要がある。例えば、図２１に示す例ではＩＰｓｅｃ処理装置２ａ、ＩＰｓｅｃ処理装置２ｂ以外にもＩＰｓｅｃ処理装置２ｄ、ＩＰｓｅｃ処理装置２ｅに対するポリシーも設定されている。

【０１５５】

続いて、ＩＰｓｅｃ設定サーバ１にはＩＰｓｅｃ処理装置２ａ、ＩＰｓｅｃ処理装置２ｂ間に適用するＩＰｓｅｃのポリシーを配布ポリシー記憶部１６に設定する。配布ポリシー記憶部１６の一例を図３に示す。配布ポリシー記憶部１６のアドレスペア欄には、ＩＰｓｅｃ処理装置２ａ、ＩＰｓｅｃ処理装置２ｂのアドレスを、配布ポリシー欄には当該通信に適用するポリシーを設定する。

【０１５６】

ポリシーでは使用するＩＰｓｅｃプロトコル、カプセル化モード、暗号化アルゴリズム、認証アルゴリズム、ＳＡの有効期間を設定する。また、ＩＰｓｅｃ設定サーバ１が共有秘密鍵を各ＩＰｓｅｃ処理装置２ａ～２ｆに配布するため、ＩＰｓｅｃ処理装置２ａ～２ｆはＩＫＥを使用しない。したがって、配布ポリシーにはＩＫＥに関するパラメータを設定する必要がない。

【０１５７】

配布ポリシー記憶部１６にはＩＰｓｅｃ設定サーバ１が管理する他の通信に対するポリシーをすべて設定しておく。図３に示す例では、ＩＰｓｅｃ処理装置２

ａ、ＩＰｓｅｃ処理装置２ｂ間の通信以外にも、ＩＰｓｅｃ処理装置２ｄ、ＩＰｓｅｃ処理装置２ｅ間の通信に対するポリシーが設定されている。

【０１５８】

各ＩＰｓｅｃ処理装置２ａ～２ｆにはＳＰＤ２４を設定する。ＳＰＤ２４にはＩＰｓｅｃ設定サーバ１との通信をＩＰｓｅｃで暗号化するために通常のＩＰｓｅｃの設定を行い、実際にＩＰｓｅｃを適用したい通信に関しては、セレクタ欄と設定要求用相手アドレス欄とを設定する。

【０１５９】

ＩＰｓｅｃ処理装置２ａのＳＰＤ２４の一例を図１５に示す。ＩＤ＝１のエントリが、ＩＰｓｅｃ設定サーバ１との通信を暗号化するための設定である。この設定はＩＰｓｅｃ設定サーバ１のＳＰＤ１３に設定したものに対応している。適用ポリシー（ｚ）の内容を図１６に示す。相手先アドレス以外はＩＰｓｅｃ設定サーバ１に設定したポリシーと同じであり、ＩＫＥに関する設定も含まれる。

【０１６０】

ＩＤ＝２のエントリがプライベートネットワーク２０２宛の通信を暗号化するための設定である。セレクタ欄には対象となる通信としてプライベートネットワーク２０２宛の通信を設定し、処理欄にはＩＰｓｅｃを設定する。ここで、ＩＰｓｅｃ適用ポリシー欄は省略し、設定要求用相手アドレス欄にＩＰｓｅｃ処理装置２ｂのアドレスを設定する。

【０１６１】

ＳＰＤ２４にはＩＰｓｅｃ処理装置２ａがＩＰｓｅｃを適用したい通信をすべて設定する。図１５に示す例では、ＩＰｓｅｃ処理装置２ｂとの通信以外にプライベートネットワーク２０３宛の通信に対してＩＰｓｅｃ処理装置２ｃとＩＰｓｅｃ通信を実施する設定となっている。

【０１６２】

ＩＰｓｅｃ処理装置２ｂにも上記と同様の設定を行う。すわなち、ＳＰＤ２４にＩＰｓｅｃ設定サーバ１用の設定を適用ポリシーとともに設定し、他のＩＰｓｅｃ通信に対してはセレクタと設定要求用相手アドレスとを設定しておく。

【０１６３】

以上が予め必要な設定となる。従来のＩＰｓｅｃ処理装置のＳＰＤに、上記と同様の設定を設定した例を図２３に示す。従来のＩＰｓｅｃ処理装置ではＩＰｓｅｃ設定サーバ１用の設定が不要となるが、ＩＰｓｅｃを適用するすべての通信についてＩＫＥに関する設定を含む適用ポリシーを設定しなければならない。図２３に示す例では、プライベートネットワーク２０２、プライベートネットワーク２０３宛の通信に対してそれぞれ適用ポリシー（ｊ）、適用ポリシー（ｋ）を設定している。適用ポリシー（ｊ）の内容を図２４に示す。適用ポリシー（ｊ）にはＩＰｓｅｃプロトコル、カプセル化モード等のＩＰｓｅｃ適用ポリシーに加えて、ＩＫＥのポリシーも設定する。

【０１６４】

ここで、ｎ台のＩＰｓｅｃ処理装置がすべての組み合わせで、互いにＩＰｓｅｃの通信を実施する場合において、本実施例によるＩＰｓｅｃ設定サーバ１を用いた場合の設定量と従来のＩＰｓｅｃ処理装置に必要な設定量とを比較する。ＩＰｓｅｃのポリシーに関する設定とＩＫＥのポリシーに関する設定とをそれぞれ「１」と数えると、従来のＩＰｓｅｃ処理装置では、１台のＩＰｓｅｃ処理装置に（ｎ－１）件分のＩＰｓｅｃポリシーとＩＫＥポリシーとを設定する必要があるため、１台当たりの設定量は２（ｎ－１）となり、ｎ台で２ｎ（ｎ－１）となる。

【０１６５】

これに対し、本実施例によるＩＰｓｅｃ処理装置２ではＩＰｓｅｃ設定サーバ１との通信用にＩＰｓｅｃポリシーとＩＫＥポリシーとを１件ずつ設定するのみで、１台当たりの設定量は２となり、ｎ台で２ｎとなる。

【０１６６】

ＩＰｓｅｃ設定サーバ１には、それぞれのＩＰｓｅｃ処理装置２との通信のためにＩＰｓｅｃポリシーとＩＫＥポリシーとを１件ずつ設定することによって２ｎの設定量と、個々のＩＰｓｅｃ処理装置２同士の通信の組合せに対してＩＰｓｅｃポリシーを１件設定するためにｎ（ｎ－１）／２の設定量とが必要となり、ＩＰｓｅｃ設定サーバ１全体に必要な設定量は２ｎ＋ｎ（ｎ－１）／２となる。

【０１６７】

したがって、本実施例によるＩＰｓｅｃ設定サーバ１を用いた場合の設定量は４ｎ＋ｎ（ｎ－１）／２＝ｎ（ｎ＋７）／２となる。例えば、ｎ＝１０の場合には従来の手法の設定量１８０に対して、本発明の設定量が８５となり、約半分の設定で済むことになる。

【０１６８】

n^2 の係数に注目すれば、ｎが大きくなると、本実施例における設定量が従来の手法の１／４に近づくことがわかり、組合せが多くなるほど効果が大きくなることがわかる。

【０１６９】

続いて、ＩＰｓｅｃ処理装置２ａがプライベートネットワーク２０２宛のパケットを受信した後の動作について説明する。ＩＰｓｅｃ処理装置２ａがプライベートネットワーク２０２宛のパケットをインタフェース部２１から受信すると、パケットはＩＰｓｅｃ処理部２３に渡される。

【０１７０】

ＩＰｓｅｃ処理部２３はＳＰＤ２４のセレクタと受信したパケットを比較して該当するエントリを探す。図１５に示す内容とプライベートネットワーク２０２宛のパケットを比較すると、ＩＤ＝２のエントリと一致する。ＩＰｓｅｃ処理部２３は該当エントリの処理欄にしたがってＩＰｓｅｃの適用を試みるが、ＩＰｓｅｃ適用ポリシーが設定されておらず、代わりに設定要求用相手アドレスが設定されているため、ＩＰｓｅｃ適用処理を一時中断し、設定管理部２６に設定の取得を依頼する。

【０１７１】

設定管理部２６はＩＰｓｅｃ処理部２３から設定取得の依頼を受けると、当該ＳＰＤエントリ用の要求メッセージを生成する。要求メッセージの例を図６に示す。ＩＤとＳＰＩとは設定管理部２６が任意の数値を設定し、要求元アドレスにはＩＰｓｅｃ処理装置２ａ自身のアドレスを、相手先アドレスにはＳＰＤエントリの設定要求用相手アドレスであるＩＰｓｅｃ処理装置２ｂのアドレスを設定する。

【０１７２】

設定管理部２６は生成した要求メッセージをＩＰｓｅｃ設定サーバ１に送信する。設定管理部２６はＩＰｓｅｃ設定サーバ１に要求メッセージを送信すると、５秒間隔で要求メッセージの送信を繰り返し、ＩＰｓｅｃ設定サーバ１から要求メッセージに対応する応答を受信するか要求メッセージを６回送信すると要求メッセージの送信を停止する。繰り返し送信することによって、１個の要求メッセージが紛失した場合にも他の要求メッセージによって処理を継続することができる。

【０１７３】

設定管理部２６からＩＰｓｅｃ設定サーバ１に要求メッセージが送信される時、要求メッセージは図１５に示すＳＰＤ２４の１番目のエントリにしたがって、ＩＰｓｅｃ処理部２３によってＩＰｓｅｃを適用されてからＩＰｓｅｃ設定サーバ１に送信される。そのため、ＩＰｓｅｃ設定サーバ１に送信されるメッセージはインタネット１００上の第３者に盗聴されることなく、安全に送信することができる。尚、各ＩＰｓｅｃ処理装置２からＩＰｓｅｃ設定サーバ１に送信されるメッセージはすべて同様の手順でＩＰｓｅｃを適用されてから送信されるため、以下の説明ではＩＰｓｅｃ設定サーバ１に送信するメッセージに対してＩＰｓｅｃを適用する手順についてはその説明を省略する。

【０１７４】

ＩＰｓｅｃ設定サーバ１に送信された要求メッセージはＩＰｓｅｃ設定サーバ１のインタフェース部１１に到着する。インタフェース部１１で受信された要求メッセージはＩＰｓｅｃ処理部１２に送られる。ＩＰｓｅｃ処理部１２ではＩＰｓｅｃによって暗号化された要求メッセージを元の状態に復号し、復号後のパケットを要求処理部１５に送る。

【０１７５】

尚、各ＩＰｓｅｃ処理装置２からＩＰｓｅｃ設定サーバ１に送られるメッセージはすべて同様の手順で要求処理部１５に届くため、以下の説明ではインタフェース部１１でメッセージが受信されてから要求処理部１５に届けられるまでの手順についてはその説明を省略する。同様に、ＩＰｓｅｃ設定サーバ１からＩＰｓｅｃ処理装置２に送信されるメッセージにＩＰｓｅｃが適用される手順について

もその説明を省略する。

【０１７６】

要求処理部１５は要求メッセージを受信すると（図１２ステップＳ１）、管理テーブル１７からアドレス及びＩＤが一致するエントリを検索するが、最初は管理テーブル１７には何も設定されていないため、一致するエントリが見つからない（図１２ステップＳ２，Ｓ７，Ｓ９）。

【０１７７】

要求処理部１５は新規登録のため、要求メッセージに含まれる要求元アドレスと相手先アドレスをキーにして配布ポリシー記憶部１６の中から該当するエントリを検索する（図１３ステップＳ２１）。要求メッセージに含まれる要求元／相手先アドレスはそれぞれＩＰｓｅｃ処理装置２ａ及びＩＰｓｅｃ処理装置２ｂなので、図３に示す配布ポリシー記憶部１６の先頭のエントリが一致する。

【０１７８】

配布ポリシー記憶部１６に一致するエントリが見つかったので、要求処理部１５は管理テーブル１７の新しいエントリを選び、要求元アドレス、相手先アドレス、要求ＩＤ、ＳＰＩ欄にそれぞれ要求メッセージに含まれるＩＰｓｅｃ処理装置２ａのアドレス、ＩＰｓｅｃ処理装置２ｂのアドレス、要求ＩＤの「１００１」、ＳＰＩの「５１００」を設定する。同一エントリのもう一つの要求元アドレス、相手先アドレスにはそれぞれＩＰｓｅｃ処理装置２ｂのアドレス、ＩＰｓｅｃ処理装置２ａのアドレスを設定する。

【０１７９】

さらに、配布ポリシー記憶部１６の該当エントリに設定されている配布ポリシー（ａ）を管理テーブル１７の設定パラメータ欄に設定する（図１３ステップＳ２２）。ここまでの設定を終えた管理テーブル１７を図２５に示す。

【０１８０】

要求処理部１５は相手先アドレスであるＩＰｓｅｃ処理装置２ｂに対して要求起動メッセージを送信する（図１３ステップＳ２３）。要求起動メッセージには、相手先アドレスとして要求メッセージの送信元アドレスであるＩＰｓｅｃ処理装置２ａのアドレスを設定する。要求起動メッセージの一例を図８に示す。

【０１８１】

要求処理部１５はＩＰｓｅｃ処理装置２ｂから要求メッセージを受信するまで、５秒間隔で最大６回要求起動メッセージを送信する。繰り返し送信することによって、１個の要求起動メッセージが紛失した場合にも他の要求起動メッセージによって処理を継続することができる。

【０１８２】

ＩＰｓｅｃ処理装置２ｂに送信された要求起動メッセージはＩＰｓｅｃ処理装置２ｂのインタフェース部２２に到着する。ＩＰｓｅｃ処理装置２ｂでは、インタフェース部２２で受信された要求起動メッセージがＩＰｓｅｃ処理部２３に送られる。

【０１８３】

ＩＰｓｅｃ処理部２３ではＩＰｓｅｃによって暗号化された要求起動メッセージを元の状態に復号し、復号後のパケットをルーティング部２７に送る。ルーティング部２７ではメッセージの宛先がＩＰｓｅｃ処理装置２ｂ自身であることを判断して、要求起動メッセージを設定管理部２６に渡す。尚、ＩＰｓｅｃ設定サーバ１から各ＩＰｓｅｃ処理装置２に送信されるメッセージはすべて同様の手順で設定管理部２６に届くため、以下の説明ではインタフェース部２２でメッセージが受信されてから設定管理部２６に届けられるまでの手順についてはその説明を省略する。

【０１８４】

設定管理部２６はＩＰｓｅｃ設定サーバ１から要求起動メッセージを受信すると、ＳＰＤ２４のエントリの中から、設定要求用相手アドレスがＩＰｓｅｃ処理装置２ａのアドレスと一致するエントリを検索する。ＩＰｓｅｃ処理装置２ｂのＳＰＤ２４には予めＩＰｓｅｃ処理装置２ａ用のエントリを設定済みであるため、そのエントリと一致する。

【０１８５】

設定管理部２６は当該エントリのポリシーを取得するために要求メッセージを生成する。要求メッセージでは要求元アドレス、相手先アドレスにそれぞれＩＰｓｅｃ処理装置２ｂ、ＩＰｓｅｃ処理装置２ａのアドレスを設定し、ＩＤ及びＳ

ＰＩにはそれぞれ設定管理部２６が任意に選択した要求ＩＤ「２００１」、ＳＰＩ「６１００」を設定する。

【０１８６】

設定管理部２６は生成した要求メッセージをＩＰｓｅｃ設定サーバ１に送信する。設定管理部２６はＩＰｓｅｃ設定サーバ１に要求メッセージを送信すると、５秒間隔で要求メッセージの送信を繰り返し、ＩＰｓｅｃ設定サーバ１から要求メッセージに対応する応答を受信するか、要求メッセージを６回送信すると、要求メッセージの送信を停止する。

【０１８７】

ＩＰｓｅｃ処理装置２ｂから送信された要求メッセージはＩＰｓｅｃ設定サーバ１のインタフェース部１１に到着し、要求処理部１５に転送される。要求処理部１５はＩＰｓｅｃ処理装置２ｂから要求メッセージを受信すると、要求起動メッセージの送信を停止し、要求メッセージの受信処理（図１２ステップＳ１）を開始する。

【０１８８】

要求処理部１５は図２５に示す管理テーブル１７から要求メッセージに含まれるアドレス及びＩＤが一致するエントリを検索するが、ＩＤが一致するエントリは存在しない（図１２ステップＳ２）。また、アドレス及びＳＰＩが一致するエントリも存在しない（図１２ステップＳ７）。

【０１８９】

続いて、要求処理部１５は管理テーブル１７においてアドレスが一致してＩＤが空欄のエントリを検索する（図１２ステップＳ９）。図２５に示す最初のエントリが該当するので、要求処理部１５は要求メッセージに含まれる値を使用して、空欄になっているＩＤ欄及びＳＰＩ欄に要求ＩＤ「２００１」、ＳＰＩ「６１００」をそれぞれ設定する。

【０１９０】

さらに、ＩＰｓｅｃ処理装置２ａからＩＰｓｅｃ処理装置２ｂへの順方向用のＳＡパラメータと、逆方向用のＳＡパラメータとを生成する（図１２ステップＳ１０）。具体的には、ＩＰｓｅｃプロトコル、カプセル化モード、暗号化アルゴ

リズム、認証アルゴリズム、有効期限について配布ポリシー（ａ）と同一の内容を設定し、暗号化鍵、認証鍵、ＩＶについては乱数生成器１８から乱数を取得して値を設定する。

【０１９１】

また、受信側ＳＰＩ欄には受信側となるＩＰｓｅｃ処理装置２が使用するＳＰＩを設定する。設定後の管理テーブル１７の内容を図４に示す。１番目のエントリについて、要求ＩＤの欄に「２００１」が設定され、ＳＰＩの欄に「６１００」が設定され、それぞれの方向用のＳＡパラメータにはＳＡパラメータ（ａ）とＳＡパラメータ（ｂ）とが設定されている。ＳＡパラメータ（ａ）の内容を図５に示す。逆方向のＳＡパラメータ（ｂ）では暗号化鍵、認証鍵、ＩＶとして異なる乱数値が使用されることと、受信側ＳＰＩの値がＩＰｓｅｃ処理装置２ａ用の「５１００」となること以外は同じ内容となる。

【０１９２】

要求処理部１５は管理テーブル１７の設定パラメータ欄の内容を使用して配布メッセージを作成し、ＩＰｓｅｃ処理装置２ａとＩＰｓｅｃ処理装置２ｂに対してそれぞれ送信する（図１２ステップＳ１１）。

【０１９３】

この時、送信する配布メッセージに設定する要求元アドレス、相手先アドレス、ＩＤは管理テーブル１７の当該エントリで示される値を使用する。したがって、ＩＰｓｅｃ処理装置２ａ宛の配布メッセージでは要求元アドレス、相手先アドレス、ＩＤの値はそれぞれＩＰｓｅｃ処理装置２ａのアドレス、ＩＰｓｅｃ処理装置２ｂのアドレス、要求ＩＤ「１００１」となり、ＩＰｓｅｃ処理装置２ｂ宛の配布メッセージではそれぞれＩＰｓｅｃ処理装置２ｂのアドレス、ＩＰｓｅｃ処理装置２ａのアドレス、要求ＩＤ「２００１」となる。ＩＰｓｅｃ処理装置２ａ宛の配布メッセージの内容を図７に示す。

【０１９４】

要求処理部１５は配布メッセージを送信後、タイマ１９を使用してＳＡパラメータの有効期限と同じ時間を計測し、タイマ１９が満了した時点で管理テーブル１７の当該エントリを削除する。

【０１９５】

ＩＰｓｅｃ設定サーバ１からＩＰｓｅｃ処理装置２ａに送信された配布メッセージはＩＰｓｅｃ処理装置２ａのインタフェース部２２に到着し、設定管理部２６に転送される。

【０１９６】

ＩＰｓｅｃ処理装置２ａの設定管理部２６はＩＰｓｅｃ設定サーバ１から配布メッセージを受信すると、要求メッセージの送信を停止し、配布メッセージに含まれる適用ポリシーをＳＰＤ２４のＩＰｓｅｃ適用ポリシー欄に設定する。ポリシーを設定した後のＳＰＤ２４の内容を図２６に示す。

【０１９７】

さらに、設定管理部２６は配布メッセージに含まれるＳＡパラメータを使用して、双方向の通信用にそれぞれＳＡを生成し、ＳＡＤ２５に設定する。ＩＰｓｅｃ処理装置２ａからＩＰｓｅｃ処理装置２ｂ方向のＳＡを設定したＳＡＤ２５の内容を図１７に示す。

【０１９８】

ＳＡＤ２５の１番目のエントリが該当エントリである。配布メッセージで通知されたＳＡパラメータ（ａ）はシーケンス番号が加えられてＳＡＤ２５に設定されている。受信用のＳＡＤ２５も配布メッセージによって通知されたＳＡパラメータ（ｂ）の内容にしたがって同様に設定する。この時点でＩＰｓｅｃ処理装置２ａのＩＰｓｅｃ処理部２３がＩＰｓｅｃ処理装置２ｂ宛の通信に対するＩＰｓｅｃの処理を実施できるようになる。

【０１９９】

設定管理部２６はＳＰＤ２４及びＳＡＤ２５の設定を終えると、ＩＰｓｅｃ処理部２３に設定完了を通知する。ＩＰｓｅｃ処理部２３は設定管理部２６から設定完了通知を受信すると、一時中断していたデータ通信パケットの処理を再開する。この時点では、ＳＰＤ２４のエントリの適用ポリシー及び対応するＳＡＤ２５のエントリが存在するため、ＩＰｓｅｃ処理部２３は従来通りのＩＰｓｅｃ処理を実施することができる。

【０２００】

ＩＰｓｅｃを適用されたパケットはＩＰｓｅｃ処理装置２ｂ宛に送信される。ＩＰｓｅｃ処理装置２ｂ側もＩＰｓｅｃ設定サーバ１から配布メッセージを受信した時点でＳＰＤ２４及びＳＡＤ２５にエントリを設定しているため、ＩＰｓｅｃ処理装置２ａからＩＰｓｅｃ適用済みパケットを受信した時点で従来の手順でＩＰｓｅｃの復号処理を実施することができる。

【０２０１】

ＩＰｓｅｃ処理装置２ｂのＩＰｓｅｃ処理部２３によって復号処理されたパケットは、インタフェース部２１からプライベートネットワーク２０２に送出される。このようにして、プライベートネットワーク２０１から送出されたパケットはプライベートネットワーク２０２に到達する。

【０２０２】

この時、さらにプライベートネットワーク２０１からプライベートネットワーク２０２宛のパケットが引き続き発生した場合について説明する。ＩＰｓｅｃ処理装置２ａのＩＰｓｅｃ処理部２３は図２６に示すＳＰＤ２４を検索し、２番目のエントリにすでにポリシーが存在することを確認し、さらに図１７に示すＳＡＤ２５を検索して１番目のエントリに当該ＳＡが存在することも確認し、当該ＳＡを使用してＩＰｓｅｃの処理を実施する。すなわち、ＩＰｓｅｃ設定サーバ１から設定パラメータを取得した後は、従来のＩＰｓｅｃと同様に動作する。

【０２０３】

続いて、ＳＡ更新時の動作について説明する。ＩＰｓｅｃ処理装置２ａのＩＰｓｅｃ処理部２３はＳＡＤ２５を監視し、有効期限が満了するエントリについてＳＡの更新を実施する。

【０２０４】

ＳＡを更新する場合、ＩＰｓｅｃ処理部２３は設定管理部２６に設定取得を依頼する。この時、ＩＰｓｅｃ処理部２３は当該ＳＡに対応するＳＰＤ２４のエントリを設定管理部２６に通知する。

【０２０５】

設定管理部２６はＩＰｓｅｃ処理部２３から設定取得の依頼を受けると、当該ＳＰＤエントリ用の要求メッセージを生成する。要求メッセージではＩＤ及びＳ

ＰＩ以外は最初に送信した要求メッセージと同一の内容を設定する。ＩＤ及びＳＰＩは新しい値を設定する。ここでは設定管理部２６がＩＤ及びＳＰＩの値としてそれぞれ「１００２」，「５１１０」を選択したものとする。

【０２０６】

設定管理部２６は生成した要求メッセージをＩＰｓｅｃ設定サーバ１に送信する。設定管理部２６はＩＰｓｅｃ設定サーバ１に要求メッセージを送信すると、５秒間隔で要求メッセージの送信を繰り返し、ＩＰｓｅｃ設定サーバ１から要求メッセージに対応する応答を受信するか、要求メッセージを６回送信すると、要求メッセージの送信を停止する。

【０２０７】

ＩＰｓｅｃ設定サーバ１に送信された要求メッセージはＩＰｓｅｃ設定サーバ１のインタフェース部１１に到着し、要求処理部１５に届けられる。要求処理部１５は要求メッセージを受信すると（図１２ステップＳ１）、管理テーブル１７からアドレス及びＩＤが一致するエントリを検索するが、ＩＤ及びＳＰＩがともに新しい値のため、一致するエントリが見つからない（図１２ステップＳ２，Ｓ７）。また、この時点ではＩＤが空欄のエントリも存在しない（図１２ステップＳ９）。

【０２０８】

これ以降は初めて要求メッセージを受信した時の動作と同じ手順となる。すなわち、要求処理部１５は配布ポリシー記憶部１６を検索し（図１３ステップＳ２１）、管理テーブル１７に新しくエントリを登録する（図１３ステップＳ２２）。この時点での管理テーブル１７の内容を図４に示す。ＩＤ及びＳＰＩ欄がそれぞれ「１００２」，「５１１０」であるエントリが２番目に追加されていることがわかる。

【０２０９】

要求処理部１５は相手先となるＩＰｓｅｃ処理装置２ｂに要求起動メッセージを送信する（図１３ステップＳ２３）。ＩＰｓｅｃ処理装置２ｂでは要求起動メッセージを受信すると、やはり新しいＩＤとＳＰＩとを設定して要求メッセージを送信する。ここでは、ＩＰｓｅｃ処理装置２ｂが新しいＩＤ、ＳＰＩとしてそ

れぞれ「２００２」，「６１１０」を選択したものとする。

【０２１０】

ＩＰｓｅｃ設定サーバ１の要求処理部１５はＩＰｓｅｃ処理装置２ｂから要求メッセージを受信すると（図１２ステップＳ１）、アドレスは一致するが、ＩＤが空欄のエントリを発見し（図１２ステップＳ９）、要求メッセージで通知されたＩＤ及びＳＰＩと、生成したＳＡパラメータとを管理テーブル１７に設定する（図１２ステップＳ１０）。この時点での管理テーブル１７の内容を図２７に示す。

【０２１１】

図２７に示す内容を図４に示す内容と比較すると、空欄だったＩＤ，ＳＰＩ欄に「２００２」，「６１１０」が設定され、ＳＡパラメータも設定されていることがわかる。さらに、要求処理部１５は管理テーブル１７の内容にしたがって配布メッセージを生成し、ＩＰｓｅｃ処理装置２ａ及びＩＰｓｅｃ処理装置２ｂに対してそれぞれ送信する　（図１２ステップＳ１１）。

【０２１２】

各ＩＰｓｅｃ処理装置２の設定管理部２６は配布メッセージを受信すると、配布メッセージで通知されたポリシーをＳＰＤ２４に設定し、通知されたＳＡパラメータからＳＡを生成してＳＡＤ２５を設定する。この時点で、新しいＳＡが利用可能となり、ＳＡの更新が完了する。

【０２１３】

ここで、ＩＰｓｅｃ処理装置２がインタフェース部２１からＩＰｓｅｃを適用する最初のパケットを受信した後、実際にＩＰｓｅｃ処理を実施してパケットをインタフェース部２２に送信するまでの処理について、従来のＩＰｓｅｃによる手順と本実施例による手順とを比較する。

【０２１４】

従来の手法では、図３２に示すように、インタフェース部４１からパケットを受信すると、ＩＰｓｅｃ処理部４３がＩＫＥによる公開鍵の演算を実施し、通信相手となるＩＰｓｅｃ処理装置と公開鍵を交換する。ＩＰｓｅｃ処理部４３はさらに秘密鍵の演算を実施し、得られた秘密鍵を用いてＩＰｓｅｃを適用し、パケ

ットをインタフェース部４２に送る。

【０２１５】

これに対し、本実施例の手順では、図２８に示すように、ＩＰｓｅｃ処理部２３がインタフェース部２１からパケットを受信すると、ＩＰｓｅｃ処理部２３は設定管理部２６に設定取得を依頼し、設定管理部２６はＩＰｓｅｃ設定サーバ１に要求メッセージを送信する。

【０２１６】

設定管理部２６はＩＰｓｅｃ設定サーバ１から配布メッセージを受信すると、ＩＰｓｅｃ処理部２３に設定完了を通知し、ＩＰｓｅｃ処理部２３はパケットにＩＰｓｅｃを適用してインタフェース部２２に送る。

【０２１７】

インタフェース部２１がパケットを受信してからＩＰｓｅｃ処理を実施してパケットをインタフェース部２２に送信するまでの時間を、従来の手順、本実施例の手順についてそれぞれＴｂ，Ｔａとする。この時、従来の手順では公開鍵及び秘密鍵の演算に時間がかかるため、Ｔｂ＞Ｔａとなり、本実施例の手順の方が早くパケットを転送できることがわかる。

【０２１８】

例えば、ＩＫＥのＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有アルゴリズムで使用するグループを１５３６ビットＭＯＤＰ（Ｍｏｄｕｌａｒ　Ｅｘｐｏｎｅｎｔｉａｔｉｏｎ　Ｇｒｏｕｐ）として５０ＭＨｚのＲＩＳＣ（Ｒｅｄｕｃｅｄ　Ｉｎｓｔｒｕｃｔｉｏｎ　Ｓｅｔ　Ｃｏｍｐｕｔｅｒ）プロセッサを使用した場合、Ｔｂは約１８秒（実測値）となるが、Ｔａは１秒未満となる。

【０２１９】

厳密には、本実施例の手順の要求メッセージは従来のＩＰｓｅｃの手順で送信されるため、この時、ＩＫＥの鍵交換が実施される場合にはＴｂ＜Ｔａとなるが、それ以降のＩＰｓｅｃ通信については相手先となるＩＰｓｅｃ処理装置２の組合せに関係なく、ＩＰｓｅｃ設定サーバ１用のＩＫＥのＳＡが有効な間はＴｂ＞Ｔａとなる。

【０２２０】

また、従来の手法においてＩＫＥの公開鍵あるいは秘密鍵の演算を実施する場合には、ＩＰｓｅｃ処理装置がＩＫＥの演算処理に集中してしまうため、ＩＰｓｅｃを適用する必要のないパケットの転送速度が低下してしまう。ＩＫＥの鍵交換処理は通信している相手毎に定期的に発生するため、ＩＰｓｅｃ通信をする相手が多いほど処理能力が低下する割合が大きくなる。

【０２２１】

それに対して本実施例の手順では、ＩＰｓｅｃ処理装置２とＩＰｓｅｃ設定サーバ１との間で定期的に鍵交換処理が発生するが、通信相手となる各ＩＰｓｅｃ処理装置２に対しては鍵交換処理を行わないため、ＩＰｓｅｃ通信をする相手が増えたとしても処理能力が低下する割合は一定である。

【０２２２】

例えば、ＩＫＥのＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵共有アルゴリズムで使用するグループを１５３６ビットＭＯＤＰ、ＩＫＥのＳＡの有効期限を１時間として５０ＭＨｚのＲＩＳＣプロセッサを使用した場合、ＩＰｓｅｃ処理装置が他の１０台のＩＰｓｅｃ処理装置との間でＩＰｓｅｃ通信を実施すると、従来の手順では１時間の間にＩＫＥの鍵交換が１０回ずつ実施されることになり、１時間当たり約１８０秒間性能が低下することになる。

【０２２３】

それに対して、本実施例の手法では、ＩＰｓｅｃ設定サーバ１との間でＩＫＥの鍵交換が実施されるのみなので、１時間当たり約１８秒間の性能低下のみとなる。

【０２２４】

ＩＫＥの演算処理速度に起因する問題を解決する既存の手段として、演算専用回路をＩＰｓｅｃ処理装置に搭載し、ＩＫＥの演算処理自体を高速化する方法がある。演算専用回路を搭載したＩＰｓｅｃ処理装置の例を図３３に示す。演算専用回路５１がＩＰｓｅｃ処理部４３に接続されている点が、図３１に示す従来のＩＰｓｅｃ処理装置４と異なる。

【０２２５】

ＩＰｓｅｃ処理部４３はＩＫＥの演算が必要になると、演算専用回路５１に演

算を依頼する。演算専用回路５１によって高速に演算が実施されるため、図３２に示す従来手法の演算処理に要する時間が短くなり、全体の速度も向上する。この手段を用いれば、ＩＫＥの演算速度に起因する問題を解決することが可能である。但し、演算専用回路５１を持たないＩＰｓｅｃ処理装置をすでに導入してしまっている場合には、ＩＰｓｅｃ処理装置そのものを演算専用回路付きのＩＰｓｅｃ処理装置に置き換える必要がある。

【０２２６】

それに対して、本実施例の方法では必要となる機能をすべてソフトウェアで実現することができるため、すでに導入済みのＩＰｓｅｃ処理装置に対してもソフトウェアのバージョンアップで機能を追加することが可能であり、既存の設備を有効活用することができる。

【０２２７】

このように、本実施例では使用するサービスやアルゴリズム等の情報をＩＰｓｅｃ設定サーバ１に一括して設定することによって、ＩＰｓｅｃ処理装置２，２ａ～２ｆがほとんどの設定をＩＰｓｅｃ設定サーバ１から取得することが可能となるため、ＩＰｓｅｃ処理装置２，２ａ～２ｆへの設定を少なくすることができる。

【０２２８】

また、本実施例では、ＩＰｓｅｃ処理装置２，２ａ～２ｆにおいてＩＫＥを使用せずに、秘密鍵を更新することによって、ＩＫＥに関する設定が不要となるので、ＩＰｓｅｃ処理装置２，２ａ～２ｆへの設定を少なくすることができる。

【０２２９】

さらに、本実施例では、ＩＰｓｅｃ設定サーバ１を用いることによって、従来、ＩＰｓｅｃを実施する両端の装置にそれぞれ同一の設定を行う必要があるが、ＩＰｓｅｃ設定サーバ１がそれぞれの装置に設定していた内容を自装置のみに設定すればよいため、ＩＰｓｅｃ処理に関する設定の総数を少なくすることができる。

【０２３０】

上記のほかに、本実施例では、要求起動メッセージを送信しているので、要求

メッセージの送信元のＩＰｓｅｃ処理装置に対向するＩＰｓｅｃ処理装置ではその送信元のＩＰｓｅｃ処理装置でのＩＰｓｅｃのポリシーの設定とほぼ同時にＩＰｓｅｃのポリシーの設定が行われることとなり、そのポリシーの設定後に、送信元のＩＰｓｅｃ処理装置がパケットを暗号化して送信すると、対向するＩＰｓｅｃ処理装置では送信元のＩＰｓｅｃ処理装置からのパケットを復号して受取ることができる。

【０２３１】

これによって、本実施例では、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信先のＩＰｓｅｃ処理装置において送信元からのパケットを取りこぼしなく受取ることができ、対向するＩＰｓｅｃ処理装置で送信元からのパケットを復号するまでの時間を大幅に短縮することができる。

【０２３２】

また、本実施例では、要求起動メッセージの送信時にそれに応答した要求メッセージが対向するＩＰｓｅｃ処理装置から送られてこなければ、送信元のＩＰｓｅｃ処理装置に対して応答なしエラーメッセージが送信されるので、送信元のＩＰｓｅｃ処理装置で対向装置の不存在を即座に認識することができる。

【０２３３】

上記と同様に、本実施例では、ＩＰｓｅｃ設定サーバ１を用いることによって、従来、ＩＰｓｅｃを実施する両端の装置に同一の設定をそれぞれ個別に設定する必要があるので、設定内容の不一致が発生する可能性があるが、ＩＰｓｅｃ設定サーバ１が両端の装置に同一の設定を配信し、設定内容の不一致が発生しなくなるため、ＩＰｓｅｃの設定不一致による接続障害がなくなる。

【０２３４】

また、本実施例では、従来、定期的に共有秘密鍵を更新するためにＩＫＥを使用した複雑な演算が必要であるが、ＩＫＥの代わりにＩＰｓｅｃ設定サーバ１から共有秘密鍵を取得することで、両端の装置が共有秘密鍵の演算を行う必要がなくなるため、ＩＫＥを使用した場合と比較して通信を開始できるまでの時間が短くなる。

【０２３５】

これと同様に、本実施例では、従来、定期的に共有秘密鍵を更新するためにＩＫＥを使用した複雑な演算が必要であるが、ＩＫＥの代わりにＩＰｓｅｃ設定サーバ１から共有秘密鍵を取得することで、両端の装置が共有秘密鍵の演算を行う必要がなくなるため、ＩＫＥを使用した場合と比較してＩＰｓｅｃ処理を実施する装置の演算負荷を軽減することができる。

【０２３６】

図２９は本発明の他の実施例によるＩＰｓｅｃ処理装置の構成を示すブロック図である。図２９においては、ＩＰｓｅｃ処理装置３がルータではなく、パーソナルコンピュータの場合の適用例を示している。

【０２３７】

本発明の他の実施例によるＩＰｓｅｃ処理装置３はインタフェース部２１を省き、上位アプリケーション部３１を設けた以外は図１４に示す本発明の一実施例によるＩＰｓｅｃ処理装置２と同様の構成となっており、同一構成要素には同一符号を付してある。また、同一構成要素の動作は本発明の一実施例と同様である。

【０２３８】

上位アプリケーション部３１はデータ通信パケットを送受信する実体であり、ルーティング部２７に接続されている。ルーティング部２７は送受信されるパケットが上位アプリケーション部３１宛なのか、設定管理部２６宛なのか、あるいはインタネット１００宛なのかを判断してパケットをそれぞれの宛先に転送する。

【０２３９】

ここで、図１におけるＩＰｓｅｃ処理装置２ｄとＩＰｓｅｃ処理装置２ｅとがパーソナルコンピュータであるものとし、ＩＰｓｅｃ処理装置２ｄからＩＰｓｅｃ処理装置２ｅに対してパケットを送信する場合について考える。

【０２４０】

ルータの場合と同様に、ＩＰｓｅｃ設定サーバ１にはＩＰｓｅｃ処理装置２ｄ、ＩＰｓｅｃ処理装置２ｅとの間にそれぞれ安全なＩＰｓｅｃの経路を確保するためにＳＰＤ１３を設定し、ＩＰｓｅｃ処理装置２ｄ、ＩＰｓｅｃ処理装置２ｅ

間に適用するＩＰｓｅｃのポリシーを配布ポリシー記憶部１６に設定する。

【０２４１】

これらＩＰｓｅｃ処理装置２ｄ，２ｅにはＳＰＤ２４を設定する。ＩＰｓｅｃ設定サーバ１との通信を暗号化するために通常のＩＰｓｅｃの設定を行い、実際にＩＰｓｅｃを適用したい通信に関しては、セレクタと設定要求用相手アドレスとを設定する。

【０２４２】

ＩＰｓｅｃ処理装置２ｄからパケットが送信される場合、パケットを送受信する実体である上位アプリケーション部３１からデータ通信パケットがルーティング部２７に渡される。ルーティング部２７ではパケットの宛先がインタネット側であることを認識して、パケットをＩＰｓｅｃ処理部２３に転送する。

【０２４３】

これ以降は、ルータの場合の実施例と同じである。すなわち、ＩＰｓｅｃ処理部２３はＳＰＤ２４のセレクタとパケットとを比較して該当するエントリを検索し、該当するエントリに示された処理がＩＰｓｅｃであれば、ＩＰｓｅｃの適用を実施する。

【０２４４】

この時、該当するエントリにＩＰｓｅｃ適用のポリシーが存在しない場合、ＩＰｓｅｃ処理部２３はパケットの処理を一時中断し、設定管理部２６に設定要求を依頼する。設定管理部２６はＩＰｓｅｃ設定サーバ１に要求メッセージを送信し、配布メッセージを受信することでＳＰＤ２４とＳＡＤ２５とを設定し、ＩＰｓｅｃ処理部２３に設定完了を通知する。ＩＰｓｅｃ処理部２３は中断していたパケットの処理を再開し、設定されたＳＡを使用してＩＰｓｅｃを適用したうえで、パケットをインタフェース部２２経由でインタネット１００に転送する。

【０２４５】

受信時もルータの場合とほぼ同様である。ＩＰｓｅｃ処理装置２ｄ，２ｅではすでに設定管理部２６によってＳＰＤ２４、ＳＡＤ２５が設定されている。インタフェース部２２経由で受信したＩＰｓｅｃ適用済みパケットはＩＰｓｅｃ処理部２３に転送される。ＩＰｓｅｃ処理部２３はＳＡＤ２５から該当するＳＡを検

索し、パケットの復号処理を行う。

【０２４６】

復号処理によって元の状態に戻ったパケットはルーティング部２７に転送される。ルーティング部２７ではパケットが上位アプリケーション部３１宛であるか、設定管理部２６宛であるかを判断し、上位アプリケーション部３１宛であれば上位アプリケーション部３１に転送する。

【０２４７】

このようにすることで、パケットの受信処理が完了する。したがって、本実施例ではＩＰｓｅｃ処理装置２ｄ，２ｅがルータの場合でもパーソナルコンピュータの場合でも適用することができる。

【０２４８】

図３０は本発明の別の実施例による配布ポリシー記憶部の記憶内容を示す図である。本発明の一実施例ではＩＰｓｅｃ設定サーバ１の配布ポリシー記憶部１０に、実際にＩＰｓｅｃ通信を行うＩＰｓｅｃ処理装置２間に適用するポリシーを個々の通信毎に設定する必要があるが、本発明の別の実施例ではいくつかの組合せについて共通のポリシーを利用することで、配布ポリシー記憶部１６に設定するポリシーの数を減らしている。尚、本発明の別の実施例によるＩＰｓｅｃ設定サーバの構成は図２に示す本発明の一実施例によるＩＰｓｅｃ設定サーバ１の構成と同様になっている。

【０２４９】

本実施例において、配布ポリシー記憶部１６は特定のアドレスの組合せに対してポリシーを設定すると同時に、任意の組合せにおけるポリシーを設定することが可能となっている。図３０に示す例では、ＩＰｓｅｃ処理装置２ｄ、ＩＰｓｅｃ処理装置２ｅ間の通信に適用するポリシーと、それ以外のすべての組合せに適用するポリシーとが設定されている。本実施例の場合、多くのＩＰｓｅｃ処理装置２が共通のポリシーを利用することで、配布ポリシー記憶部１６に設定するポリシーの数を減らすことができる。

【０２５０】

ここで、ｎ台のＩＰｓｅｃ処理装置がすべての組合せで、互いにＩＰｓｅｃの

通信を実施する場合において、本実施例に必要な設定量と従来のＩＰｓｅｃ処理装置に必要な設定量とを比較する。この時、すべてのＩＰｓｅｃ通信の組合せにおいて同一のポリシーを適用することとする。

【０２５１】

従来のＩＰｓｅｃ処理装置に必要な設定量の合計は先に計算した通り、２ｎ（ｎ－１）である。それに対し、本実施例においては、ＩＰｓｅｃ処理装置同士の通信の組合せの数に関わらず、ＩＰｓｅｃポリシーの設定量は１件だけでよい。したがって、本実施例において必要となる設定量は４ｎ＋１となる。

【０２５２】

これからわかる通り、従来の手法では設定量がｎの２乗に比例して多くなるが、本実施例では設定量がｎに比例して大きくなるため、組合せが多くなるほど効果が大きくなることがわかる。例えば、ｎ＝１０の場合には、従来の手法の設定量が１８０に対して、本実施例の設定量が４１となり、約１／４の設定で済むことがわかる。

【０２５３】

【発明の効果】

以上説明したように本発明の装置及び方法は、ＩＰｓｅｃ処理装置間に適用するＩＰｓｅｃのポリシーを一括管理することによって、通信する装置間での設定不一致を防止することができるという効果が得られる。

【０２５４】

また、本発明の他の装置及び方法は、要求メッセージを受信した場合に当該要求メッセージを送信したＩＰｓｅｃ処理装置の通信相手であるＩＰｓｅｃ処理装置に対して当該通信用の要求メッセージを送信させるために要求起動メッセージを送信することによって、ポリシー設定後の暗号化や復号を滞りなく行うことができ、送信元からのパケットを取りこぼしなく受取ることができるという効果が得られる。

【０２５５】

さらに、本発明の別の装置及び方法は、ＩＰｓｅｃの暗号化や認証に使用するための共有秘密鍵を生成し、その生成した共有秘密鍵をＩＰｓｅｃ処理装置に配

布することによって、共有秘密鍵演算を不要とし、個々の装置での通信開始時のＩＰｓｅｃ経路の接続時間を短縮することができ、性能の低下を防ぐことができるという効果が得られる。

【図面の簡単な説明】

【図１】

本発明の一実施例によるＩＰｓｅｃによるネットワークの構成を示すブロック図である。

【図２】

図１のＩＰｓｅｃ設定サーバの構成を示すブロック図である。

【図３】

図２の配布ポリシー記憶部の記憶内容を示す図である。

【図４】

図２の管理テーブルの記憶内容を示す図である。

【図５】

図４のＳＡパラメータの内容を示す図である。

【図６】

本発明の一実施例による要求メッセージの一例を示す図である。

【図７】

本発明の一実施例による配布メッセージの一例を示す図である。

【図８】

本発明の一実施例による要求起動メッセージの一例を示す図である。

【図９】

本発明の一実施例による該当なしエラーメッセージの一例を示す図である。

【図１０】

本発明の一実施例による内容不一致エラーメッセージの一例を示す図である。

【図１１】

本発明の一実施例による応答なしエラーメッセージの一例を示す図である。

【図１２】

本発明の一実施例によるＩＰｓｅｃ設定サーバの動作を示すフローチャートで

ある。

【図１３】

本発明の一実施例によるＩＰｓｅｃ設定サーバの動作を示すフローチャートである。

【図１４】

図１のＩＰｓｅｃ処理装置の構成を示すブロック図である。

【図１５】

図１４のＳＰＤの内容を示す図である。

【図１６】

図１５に示すＳＰＤの適用ポリシー（ｚ）の一例を示す図である。

【図１７】

図１４のＳＡＤの内容を示す図である。

【図１８】

図１４のＩＰｓｅｃ処理部の処理動作を示すフローチャートである。

【図１９】

図１４の設定管理部の処理動作を示すフローチャートである。

【図２０】

図１４の設定管理部の処理動作を示すフローチャートである。

【図２１】

図２のＳＰＤの内容の一例を示す図である。

【図２２】

図２１に示すＳＰＤの適用ポリシー（ｖ）の内容を示す図である。

【図２３】

従来のＩＰｓｅｃ処理装置のＳＰＤの内容を示す図である。

【図２４】

図２３のＳＰＤの適用ポリシー（ｊ）の内容を示す図である。

【図２５】

図２の管理テーブルのＩＰｓｅｃ処理装置から要求メッセージを受信した後の内容を示す図である。

【図２６】

図１４のＳＰＤの配布メッセージを受信して適用ポリシーを設定した後の内容を示す図である。

【図２７】

図２の管理テーブルのＳＡを更新するために新しいエントリが生成される場合の内容を示す図である。

【図２８】

本発明の一実施例によるＩＰｓｅｃ処理装置の動作を示すシーケンスチャートである。

【図２９】

本発明の他の実施例によるＩＰｓｅｃ処理装置の構成を示すブロック図である。

【図３０】

本発明の別の実施例による配布ポリシー記憶部の記憶内容を示す図である。

【図３１】

従来のＩＰｓｅｃ処理装置の構成を示すブロック図である。

【図３２】

従来のＩＰｓｅｃ処理装置の動作を示すシーケンスチャートである。

【図３３】

従来のＩＰｓｅｃ処理装置の他の構成を示すブロック図である。

【符号の説明】

１　ＩＰｓｅｃ設定サーバ

２，２ａ～２ｆ，３　ＩＰｓｅｃ処理装置

１１，２１，２２　インタフェース部

１２，２３　ＩＰｓｅｃ処理部

１３，２４　ＳＰＤ

１４，２５　ＳＡＤ

１５　要求処理部

１６　配布ポリシー記憶部

１７　管理テーブル

１８　乱数生成器

１９　タイマ

２０，２８　記録媒体

２６　設定管理部

２７　ルーティング部

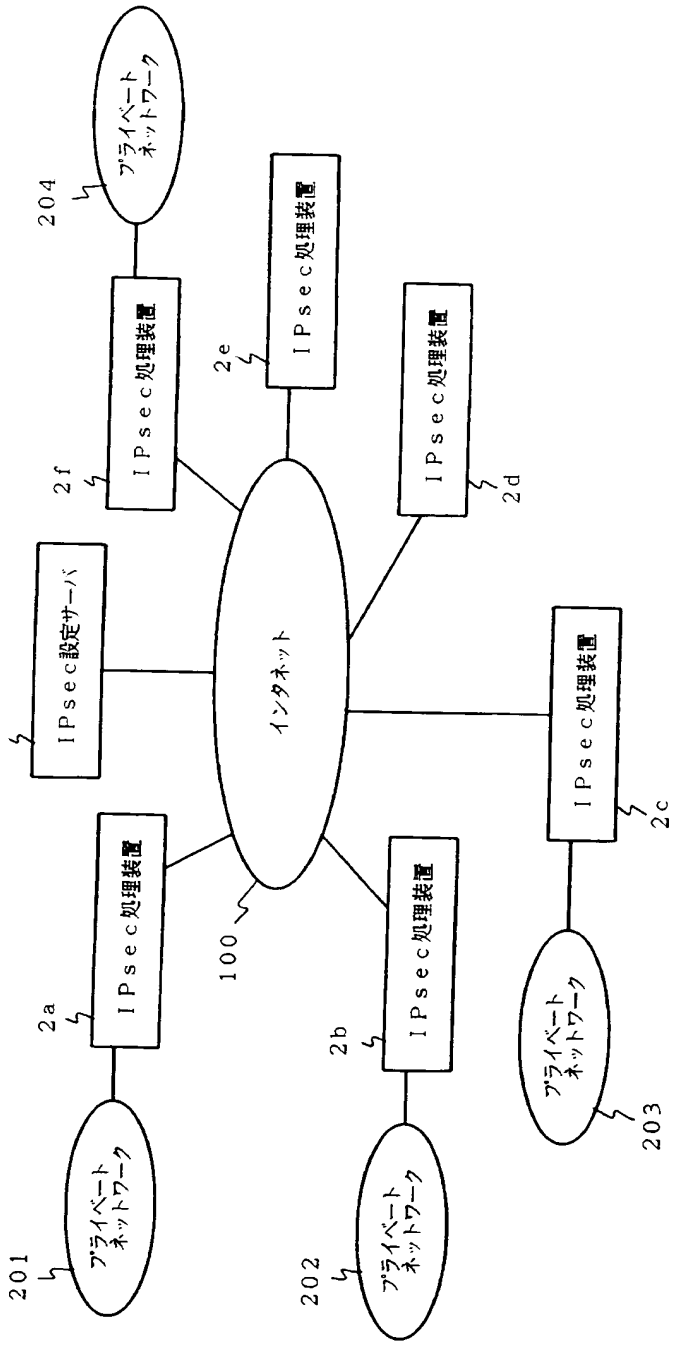
３１　上位アプリケーション部

１００　インタネット

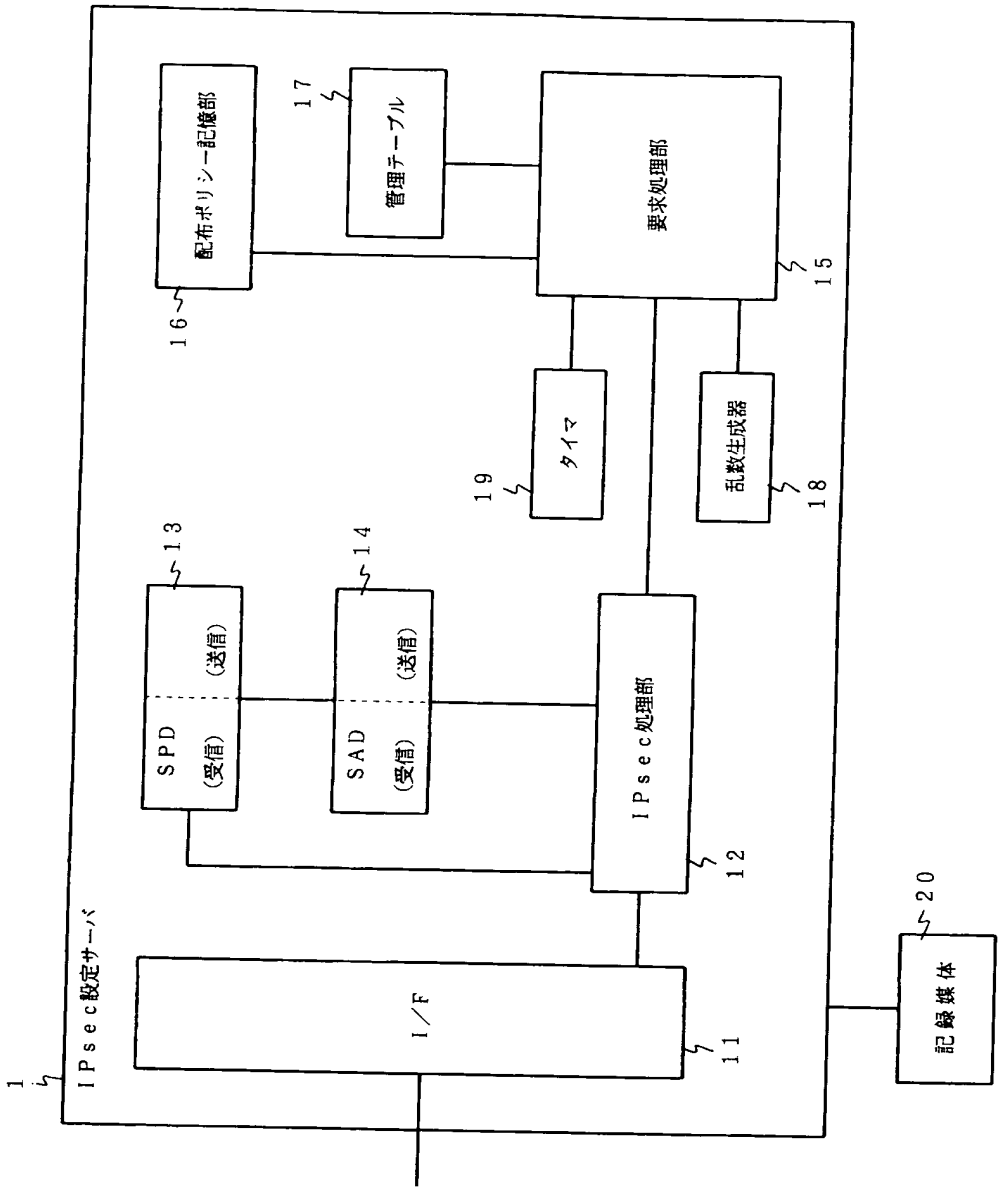
２０１～２０４　プライベートネットワーク

【書類名】　図面

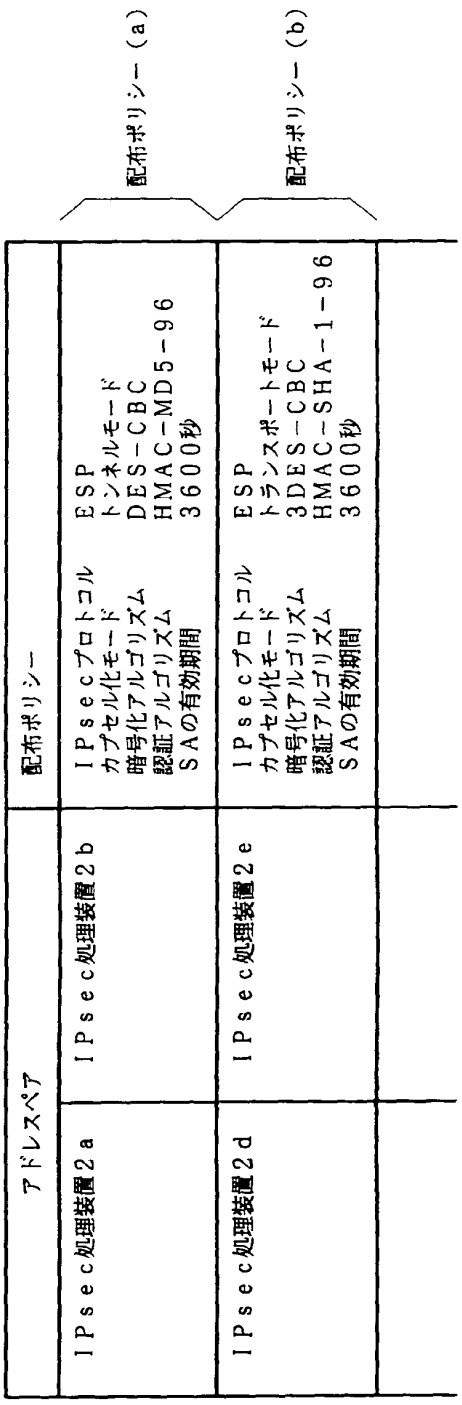
【図１】


プライベート
ネットワーク
204
IPsec処理装置
2f
IPsec処理装置
2e
IPsec処理装置
2d
IPsec設定サーバ
1
インタネット
100
IPsec処理装置
2c
IPsec処理装置
2a
IPsec処理装置
2b
プライベート
ネットワーク
201
プライベート
ネットワーク
202
プライベート
ネットワーク
203

【図２】


IPsec設定サーバ
1
I/F
11
IPsec処理部
12
SPD
(受信)
(送信)
13
SAD
(受信)
(送信)
14
タイマ
19
乱数生成器
18
要求処理部
15
管理テーブル
17
配布ポリシー記憶部
16
記録媒体
20

【図３】


アドレスペア
配布ポリシー
ＩＰｓｅｃ処理装置２ａ
ＩＰｓｅｃ処理装置２ｂ
ＩＰｓｅｃ処理装置２ｄ
ＩＰｓｅｃ処理装置２ｅ
ＩＰｓｅｃプロトコル　ＥＳＰ
カプセル化モード　トンネルモード
暗号化アルゴリズム　ＤＥＳ－ＣＢＣ
認証アルゴリズム　ＨＭＡＣ－ＭＤ５－９６
ＳＡの有効期間　３６００秒
配布ポリシー（a）
ＩＰｓｅｃプロトコル　ＥＳＰ
カプセル化モード　トランスポートモード
暗号化アルゴリズム　３ＤＥＳ－ＣＢＣ
認証アルゴリズム　ＨＭＡＣ－ＳＨＡ－１－９６
ＳＡの有効期間　３６００秒
配布ポリシー（b）

【図４】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ
1	IPsec処理装置2a	IPsec処理装置2b	1001	5100	適用ポリシー　配布ポリシー（a） 2a→2b用SAパラメータ　SAパラメータ（a） 2b→2a用SAパラメータ　SAパラメータ（b）
	IPsec処理装置2b	IPsec処理装置2a	2001	6100	
2	IPsec処理装置2a	IPsec処理装置2b	1002	5110	適用ポリシー　配布ポリシー（a） 2a→2b用SAパラメータ 2b→2a用SAパラメータ
	IPsec処理装置2b	IPsec処理装置2a			
3					

【図５】

ＩＰｓｅｃプロトコル	ＥＳＰ
カプセル化モード	トンネルモード
暗号化アルゴリズム	ＤＥＳ－ＣＢＣ
認証アルゴリズム	ＨＭＡＣ－ＭＤ５－９６
有効期限	３６００秒
暗号化鍵	０ｘ７ｄ５ｅ８３７ａｄ．．．
認証鍵	０ｘ８９ｅ５６２ｂｆｃ．．．
ＩＶ	０ｘｃ３２ｆｂｅ００４．．．
受信側ＳＰＩ	６１００

【図６】

メッセージタイプ	要求メッセージ
ＩＤ	１００１
要求元アドレス	ＩＰｓｅｃ処理装置２ａ
相手先アドレス	ＩＰｓｅｃ処理装置２ｂ
ＳＰＩ	５１００

【図７】

メッセージタイプ	配布メッセージ
ＩＤ	１００１
要求元アドレス	ＩＰｓｅｃ処理装置２ａ
相手先アドレス	ＩＰｓｅｃ処理装置２ｂ
設定パラメータ	
運用ポリシー	配布ポリシー（ａ）
２ａ→２ｂ用ＳＡパラメータ	ＳＡパラメータ（ａ）
２ｂ→２ａ用ＳＡパラメータ	ＳＡパラメータ（ｂ）

【図８】

メッセージタイプ	要求起動メッセージ
相手先アドレス	ＩＰｓｅｃ処理装置２ａ

【図９】

メッセージタイプ	該当なしエラーメッセージ
ＩＤ	１００１
要求元アドレス	ＩＰｓｅｃ処理装置２ａ
相手先アドレス	ＩＰｓｅｃ処理装置２ｂ

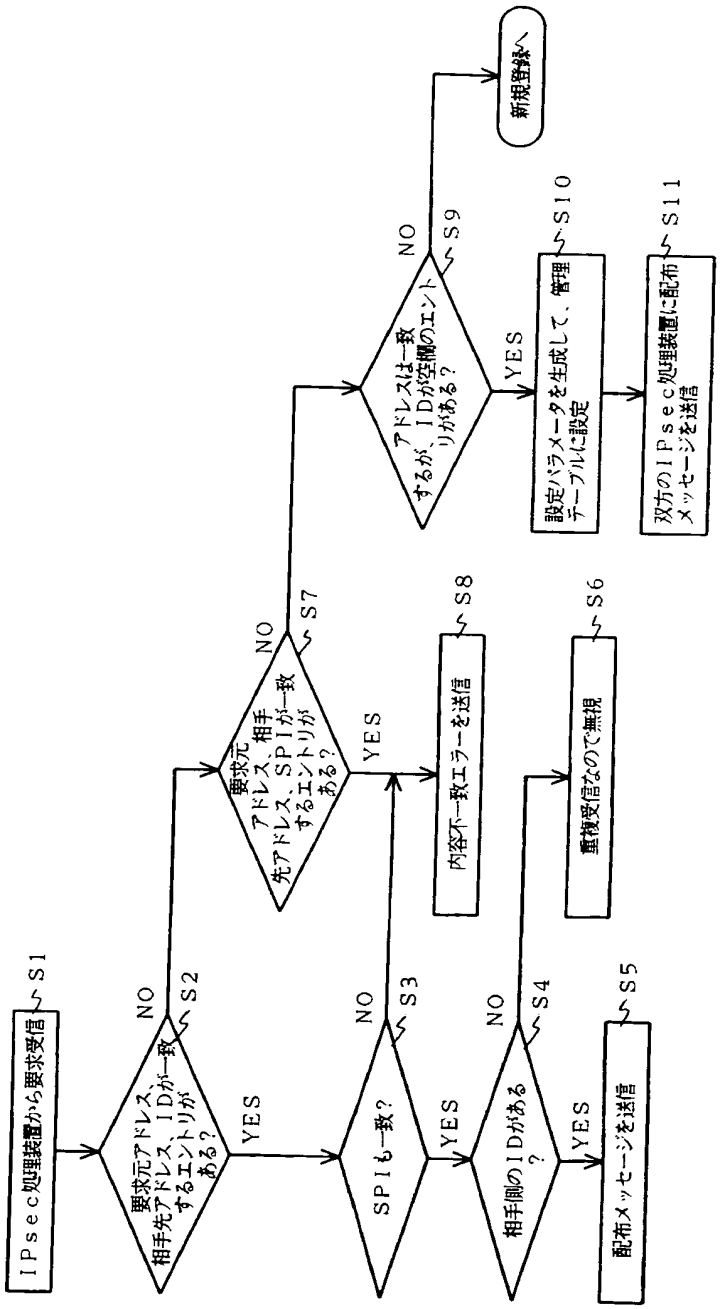
【図１０】

メッセージタイプ	内容不一致エラーメッセージ	
ＩＤ	１００１	
要求元アドレス	ＩＰｓｅｃ処理装置２ａ	
相手先アドレス	ＩＰｓｅｃ処理装置２ｂ	
エントリー一覧	ＩＤ	ＳＰＩ
	１００１	５１００
	１００２	５１１０

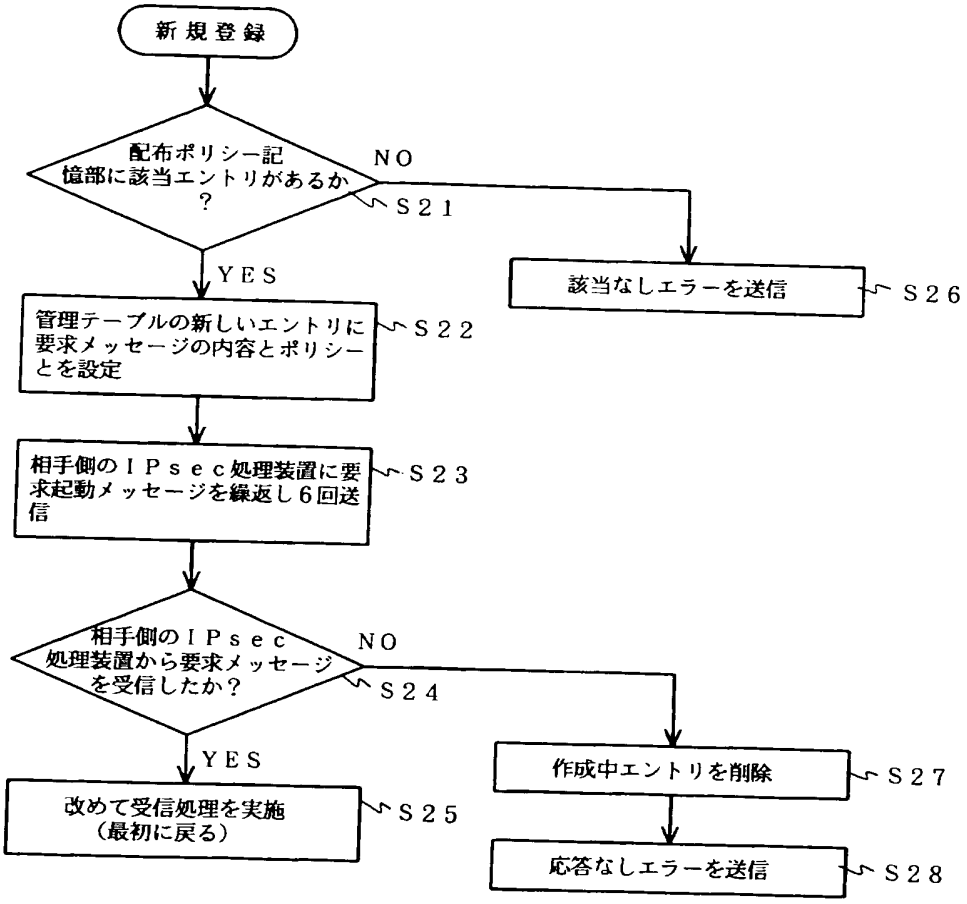
【図１１】

メッセージタイプ	応答なしエラーメッセージ
ＩＤ	１００１
要求元アドレス	ＩＰｓｅｃ処理装置２ａ
相手先アドレス	ＩＰｓｅｃ処理装置２ｂ

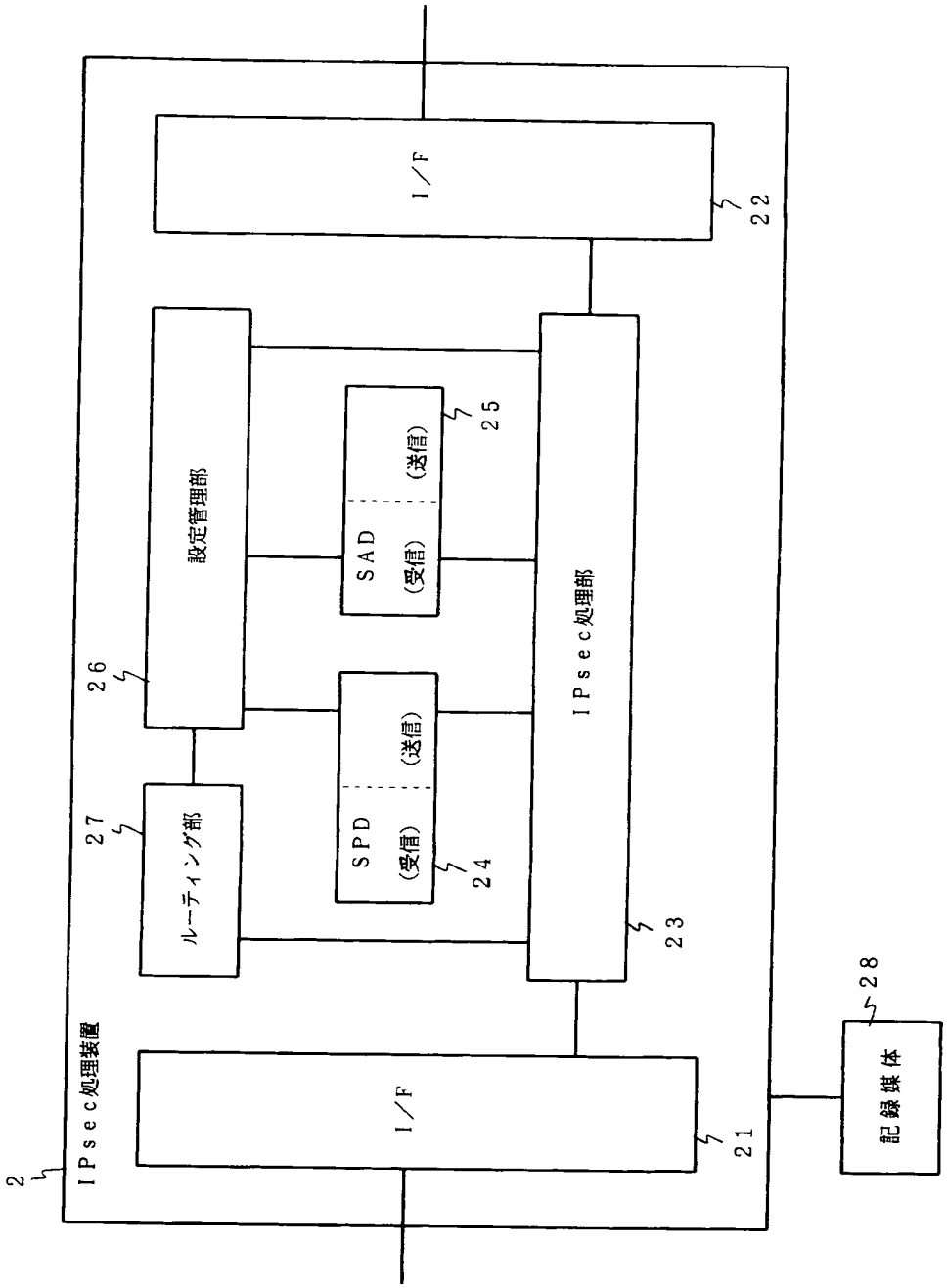
【図１２】


IPsec処理装置から要求受信
S1
要求元アドレス、相手先アドレス、IDが一致するエントリがある？
S2
NO
YES
SPIも一致？
S3
NO
YES
相手側のIDがある？
S4
NO
YES
配布メッセージを送信
S5
重複受信なので無視
S6
内容不一致エラーを送信
S8
要求元アドレス、相手先アドレス、SPIが一致するエントリがある？
S7
NO
YES
アドレスは一致するが、IDが空欄のエントリがある？
S9
NO
YES
新規登録へ
設定パラメータを生成して、管理テーブルに設定
S10
双方のIPsec処理装置に配布メッセージを送信
S11

【図１３】


新規登録
配布ポリシー記憶部に該当エントリがあるか？
NO
S21
YES
該当なしエラーを送信
S26
管理テーブルの新しいエントリに要求メッセージの内容とポリシーとを設定
S22
相手側のＩＰｓｅｃ処理装置に要求起動メッセージを繰返し６回送信
S23
相手側のＩＰｓｅｃ処理装置から要求メッセージを受信したか？
NO
S24
YES
作成中エントリを削除
S27
改めて受信処理を実施（最初に戻る）
S25
応答なしエラーを送信
S28

【図１４】


IPsec処理装置
2
I/F
21
I/F
22
IPsec処理部
23
SPD
(受信)
(送信)
24
SAD
(受信)
(送信)
25
設定管理部
26
ルーティング部
27
記録媒体
28

【図１５】

ＩＤ	セレクタ	処理	ＩＰｓｅｃ適用ポリシー	設定要求用相手アドレス
1	自分自身→設定サーバ1	ＩＰｓｅｃ	適用ポリシー（ｚ）	
2	プライベート２０２宛	ＩＰｓｅｃ		ＩＰｓｅｃ処理装置２ｂ
3	プライベート２０３宛	ＩＰｓｅｃ		ＩＰｓｅｃ処理装置２ｃ
4	上記以外すべて	通過		

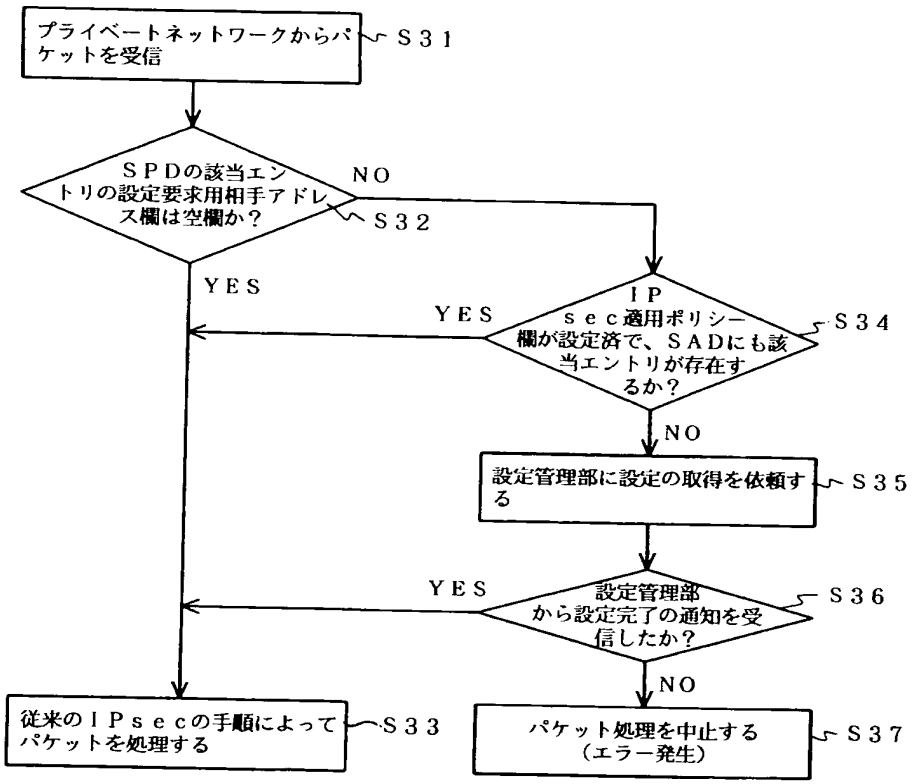
【図１６】

ＩＰｓｅｃ適用ポリシー	
ＩＰｓｅｃプロトコル	ＥＳＰ
カプセル化モード	トランスポートモード
相手先アドレス	設定サーバ1
暗号化アルゴリズム	ＡＥＳ－ＣＢＣ
認証アルゴリズム	ＨＭＡＣ－ＳＨＡ－１－９６
ＳＡの有効期間	３６００秒
ＩＫＥポリシー	
相手ＩＰｓｅｃ処理装置アドレス	設定サーバ1
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	ｐａｓｓｗｏｒｄ－ｆｏｒ－ｉｋｅ
暗号化アルゴリズム	ＤＥＳ－ＣＢＣ
ハッシュアルゴリズム	ＭＤ５
Ｏａｋｌｅｙグループ	１５３６ビットＭＯＤＰグループ
ＳＡの有効期間	３６００秒

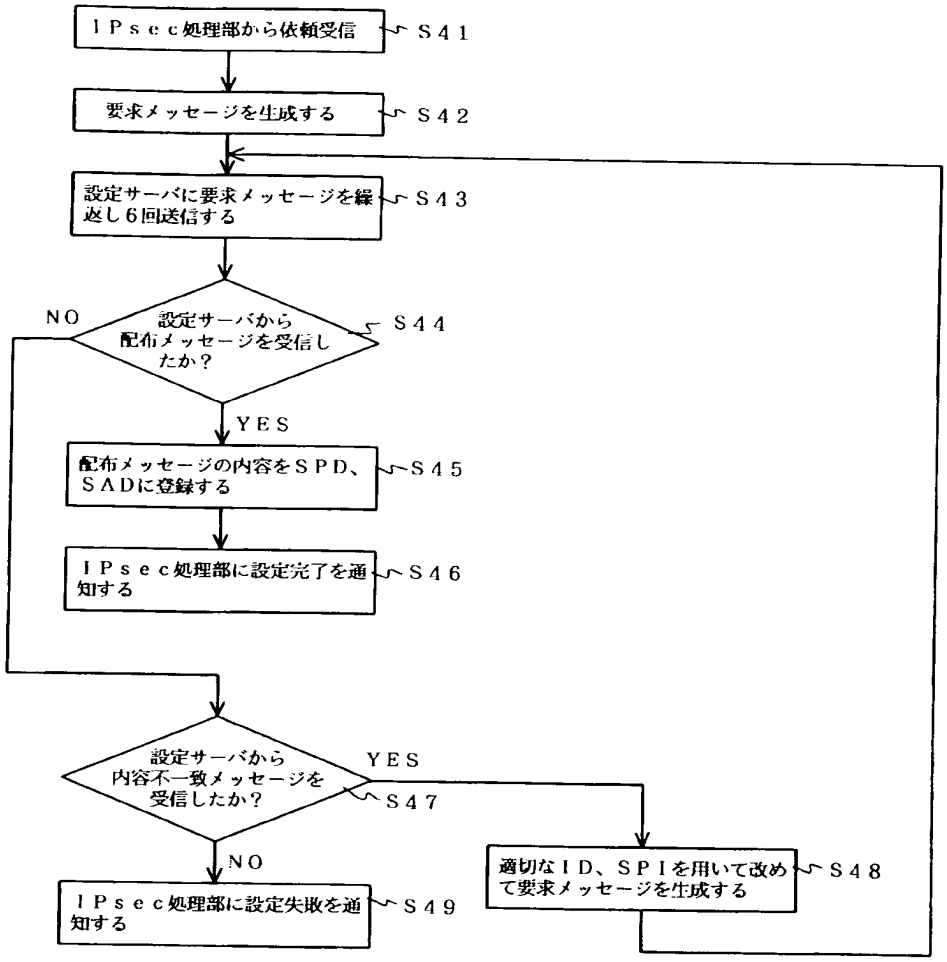
【図１７】

ID	キーパラメータ			SAパラメータ	
	終点アドレス	IPsec	SPI		
1	IPsec処理装置2b	ESP	6100	カプセル化モード	トンネルモード
				暗号化アルゴリズム	DES-CBC
				認証アルゴリズム	HMAC-MD5-96
				暗号化鍵	0x7d5e837ad...
				認証鍵	0x83e562bfc...
				IV	0xc32fbe004...
				有効期限	3600秒
				シーケンス番号	0
2	設定サーバ1	ESP	6100	カプセル化モード	トランスポートモード
				暗号化アルゴリズム	AES-CBC
				認証アルゴリズム	HMAC-SHA-1-96
				暗号化鍵	0xda738e5d7...
				認証鍵	0xcfb265e98...
				IV	0xc399ebf22...
				有効期限	3600秒
				シーケンス番号	2133
3					

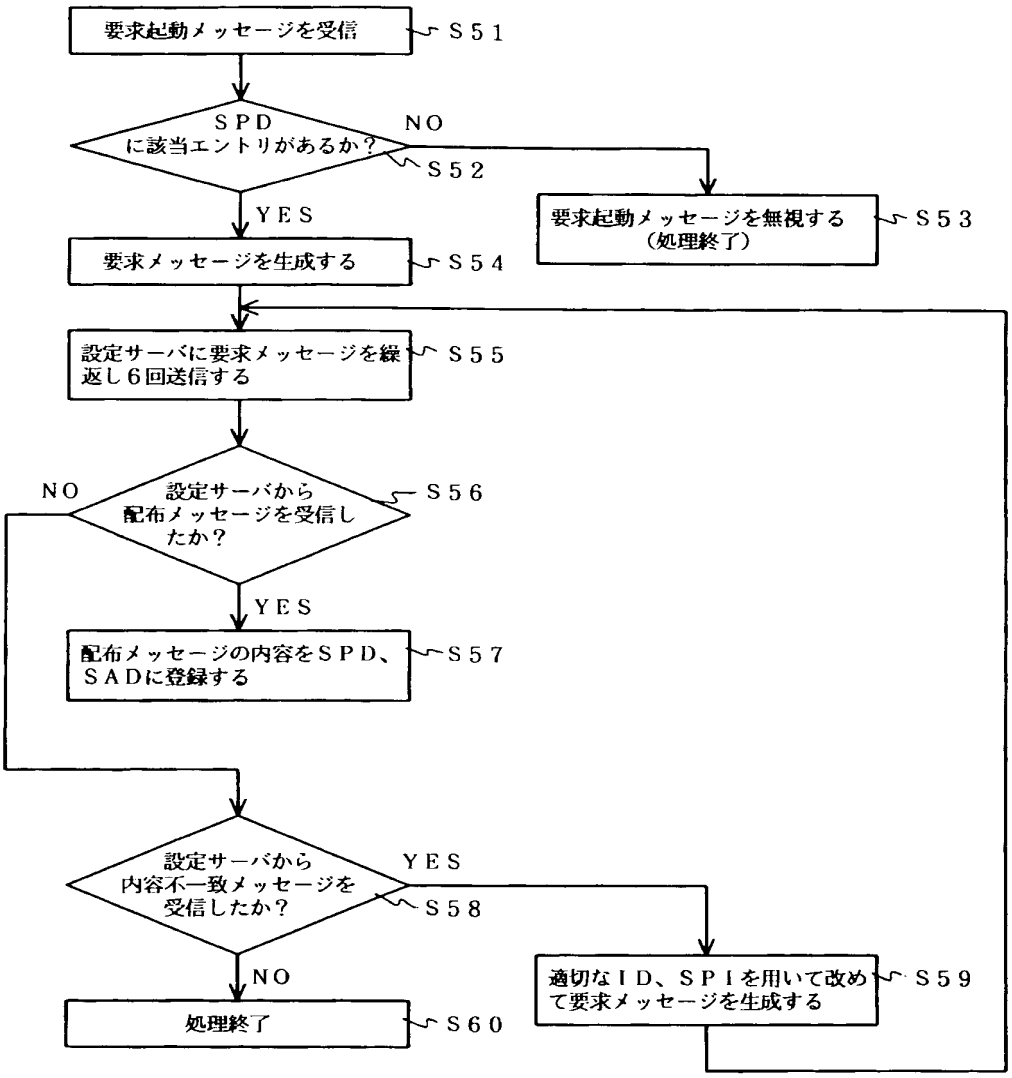
【図１８】


プライベートネットワークからパケットを受信
S31
SPDの該当エントリの設定要求用相手アドレス欄は空欄か？
NO
S32
YES
IPsec適用ポリシー欄が設定済で、SADにも該当エントリが存在するか？
YES
S34
NO
設定管理部に設定の取得を依頼する
S35
設定管理部から設定完了の通知を受信したか？
YES
S36
NO
従来のIPsecの手順によってパケットを処理する
S33
パケット処理を中止する（エラー発生）
S37

【図１９】


ＩＰｓｅｃ処理部から依頼受信
Ｓ４１
要求メッセージを生成する
Ｓ４２
設定サーバに要求メッセージを繰返し６回送信する
Ｓ４３
設定サーバから配布メッセージを受信したか？
Ｓ４４
ＮＯ
ＹＥＳ
配布メッセージの内容をＳＰＤ、ＳＡＤに登録する
Ｓ４５
ＩＰｓｅｃ処理部に設定完了を通知する
Ｓ４６
設定サーバから内容不一致メッセージを受信したか？
Ｓ４７
ＹＥＳ
ＮＯ
適切なＩＤ、ＳＰＩを用いて改めて要求メッセージを生成する
Ｓ４８
ＩＰｓｅｃ処理部に設定失敗を通知する
Ｓ４９

【図２０】


要求起動メッセージを受信
S51
SPD
に該当エントリがあるか？
NO
S52
要求起動メッセージを無視する
（処理終了）
S53
YES
要求メッセージを生成する
S54
設定サーバに要求メッセージを繰返し６回送信する
S55
NO
設定サーバから
配布メッセージを受信したか？
S56
YES
配布メッセージの内容をSPD、SADに登録する
S57
設定サーバから
内容不一致メッセージを
受信したか？
YES
S58
NO
処理終了
S60
適切なID、SPIを用いて改めて要求メッセージを生成する
S59

【図２１】

ＩＤ	セレクタ	処理	ＩＰｓｅｃ適用ポリシー
1	ＩＰｓｅｃ設定サーバ1→ＩＰｓｅｃ処理装置２ａ	ＩＰｓｅｃ	適用ポリシー（ｖ）
2	ＩＰｓｅｃ設定サーバ1→ＩＰｓｅｃ処理装置２ｂ	ＩＰｓｅｃ	適用ポリシー（ｗ）
3	ＩＰｓｅｃ設定サーバ1→ＩＰｓｅｃ処理装置２ｃ	ＩＰｓｅｃ	適用ポリシー（ｘ）
4	ＩＰｓｅｃ設定サーバ1→ＩＰｓｅｃ処理装置２ｄ	ＩＰｓｅｃ	適用ポリシー（ｙ）
5	上記以外すべて	廃棄	

【図２２】

ＩＰｓｅｃ適用ポリシー	
ＩＰｓｅｃプロトコル	ＥＳＰ
カプセル化モード	トランスポートモード
相手先アドレス	ＩＰｓｅｃ処理装置２ａ
暗号化アルゴリズム	ＡＥＳ－ＣＢＣ
認証アルゴリズム	ＨＭＡＣ－ＳＨＡ－１－９６
ＳＡの有効期間	３６００秒
ＩＫＥポリシー	
相手ＩＰｓｅｃ処理装置アドレス	ＩＰｓｅｃ処理装置２ａ
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	ｐａｓｓｗｏｒｄ－ｆｏｒ－ｉｋｅ
暗号化アルゴリズム	ＤＥＳ－ＣＢＣ
ハッシュアルゴリズム	ＭＤ５
Ｏａｋｌｅｙグループ	１５３６ビットＭＯＤＰグループ
ＳＡの有効期間	３６００秒

【図２３】

ＩＤ	セレクタ	処理	ＩＰｓｅｃ適用ポリシー
1	プライベート２０２宛	ＩＰｓｅｃ	適用ポリシー（ｊ）
2	プライベート２０３宛	ＩＰｓｅｃ	適用ポリシー（ｋ）
3	上記以外すべて	通過	

【図２４】

ＩＰｓｅｃ適用ポリシー	
ＩＰｓｅｃプロトコル	ＥＳＰ
カプセル化モード	トンネルモード
相手先アドレス	ＩＰｓｅｃ処理装置２ｂ
暗号化アルゴリズム	ＤＥＳ－ＣＢＣ
認証アルゴリズム	ＨＭＡＣ－ＭＤ５－９６
ＳＡの有効期間	３６００秒
ＩＫＥポリシー	
相手ＩＰｓｅｃ処理装置アドレス	ＩＰｓｅｃ処理装置２ｂ
相手認証方式	事前共有秘密鍵
事前共有秘密鍵	ｐａｓｓｗｏｒｄ
暗号化アルゴリズム	ＤＥＳ－ＣＢＣ
ハッシュアルゴリズム	ＭＤ５
Ｏａｋｌｅｙグループ	１５３６ビットＭＯＤＰグループ
ＳＡの有効期間	３６００秒

【図２５】

ＩＤ	要求元アドレス	相手先アドレス	要求ＩＤ	ＳＰＩ	設定パラメータ
1	ＩＰｓｅｃ処理装置２ａ	ＩＰｓｅｃ処理装置２ｂ	１００１	５１００	適用ポリシー　配布ポリシー（ａ） ２ａ→２ｂ用ＳＡパラメータ ２ｂ→２ａ用ＳＡパラメータ
	ＩＰｓｅｃ処理装置２ｂ	ＩＰｓｅｃ処理装置２ａ			
2					適用ポリシー
3					

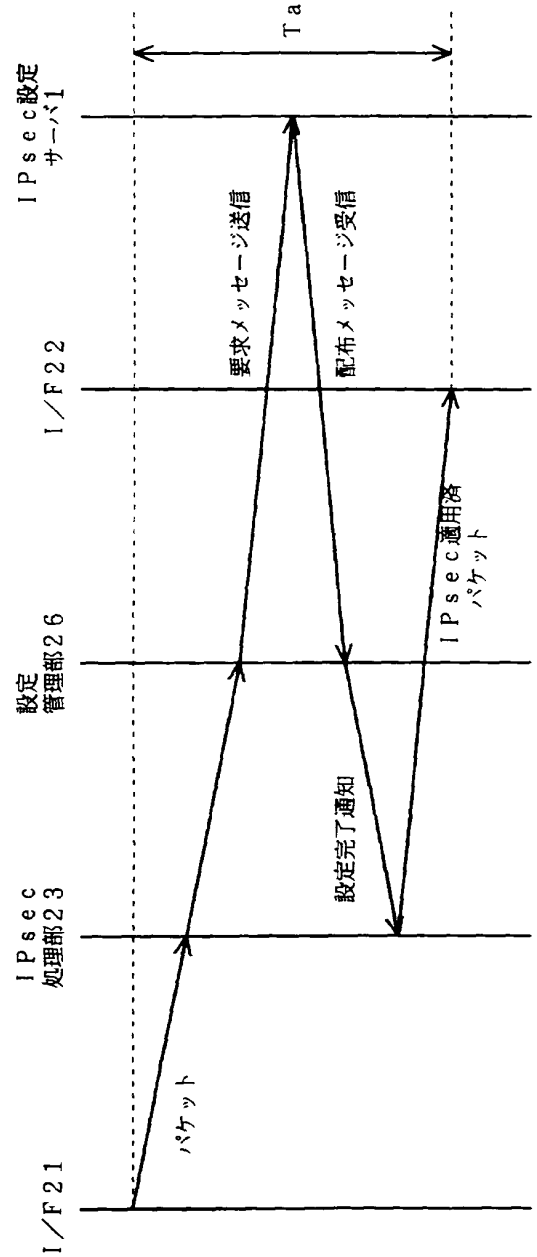
【図２６】

ＩＤ	セレクタ	処理	ＩＰｓｅｃ適用ポリシー	設定要求用相手アドレス
1	自分自身→設定サーバ１	ＩＰｓｅｃ	適用ポリシー（ｚ）	
2	プライベート２０２宛	ＩＰｓｅｃ	適用ポリシー（ａ）	ＩＰｓｅｃ処理装置２ｂ
3	プライベート２０３宛	ＩＰｓｅｃ		ＩＰｓｅｃ処理装置２ｃ
4	上記以外すべて	通過		

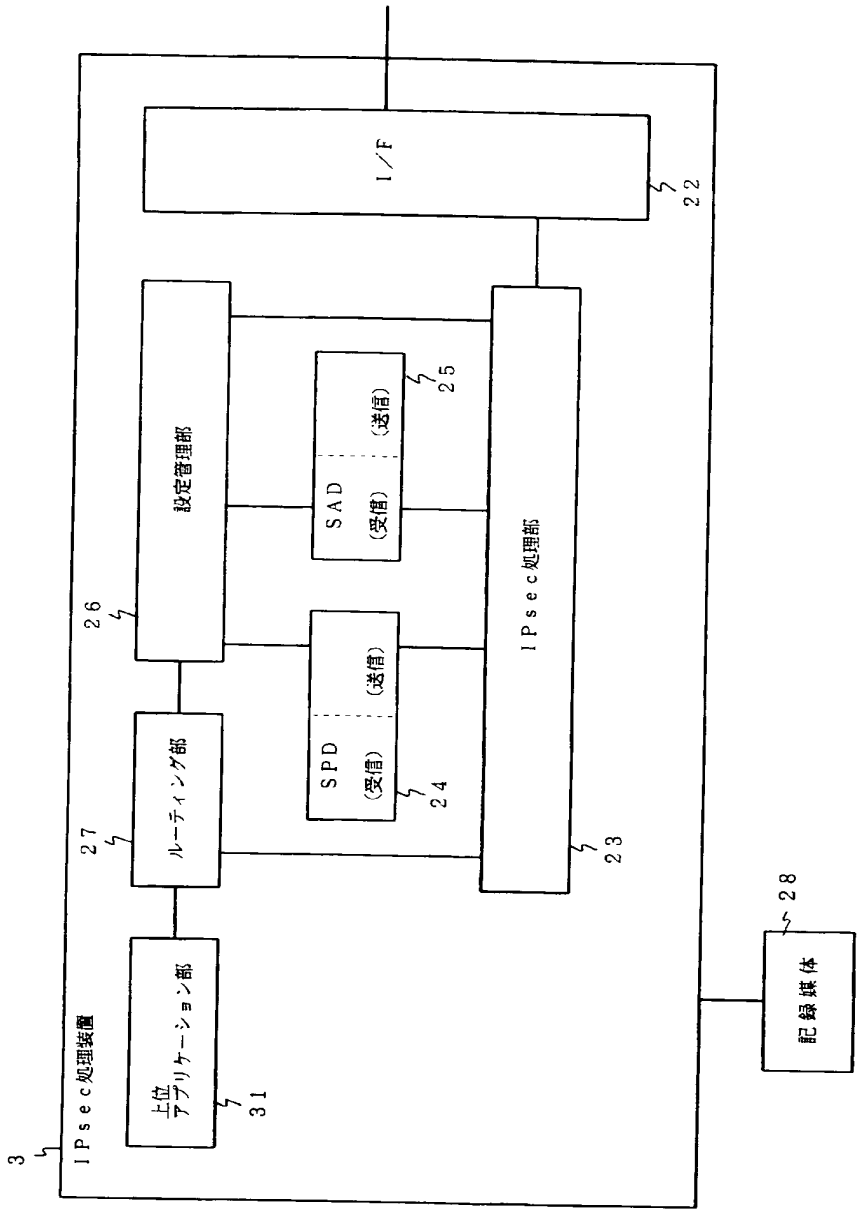
【図２７】

ID	要求元アドレス	相手先アドレス	要求ID	SPI	設定パラメータ
1	IPsec 処理装置2a	IPsec 処理装置2b	1001	5100	適用ポリシー　配布ポリシー（a） 2a→2b用SAパラメータ　SAパラメータ（a） 2b→2a用SAパラメータ　SAパラメータ（b）
	IPsec 処理装置2b	IPsec 処理装置2a	2001	6100	
2	IPsec 処理装置2a	IPsec 処理装置2b	1002	5110	適用ポリシー　配布ポリシー（a） 2a→2b用SAパラメータ　SAパラメータ（c） 2b→2a用SAパラメータ　SAパラメータ（d）
	IPsec 処理装置2b	IPsec 処理装置2a	2002	6110	
3					

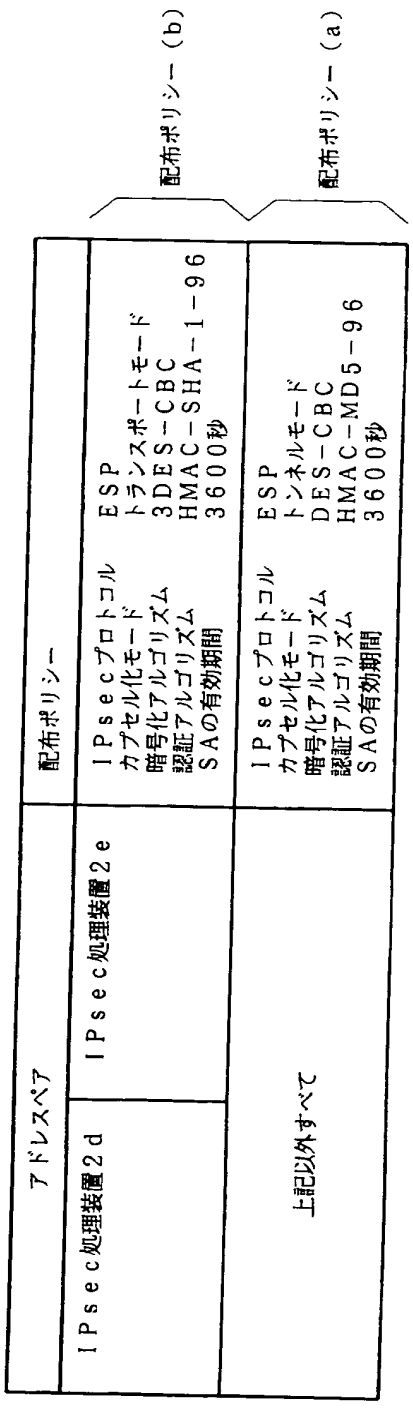
【図２８】


Ta
IPsec設定
サーバ1
I／F22
要求メッセージ送信
配布メッセージ受信
IPsec適用済
パケット
設定
管理部26
設定完了通知
IPsec
処理部23
パケット
I／F21

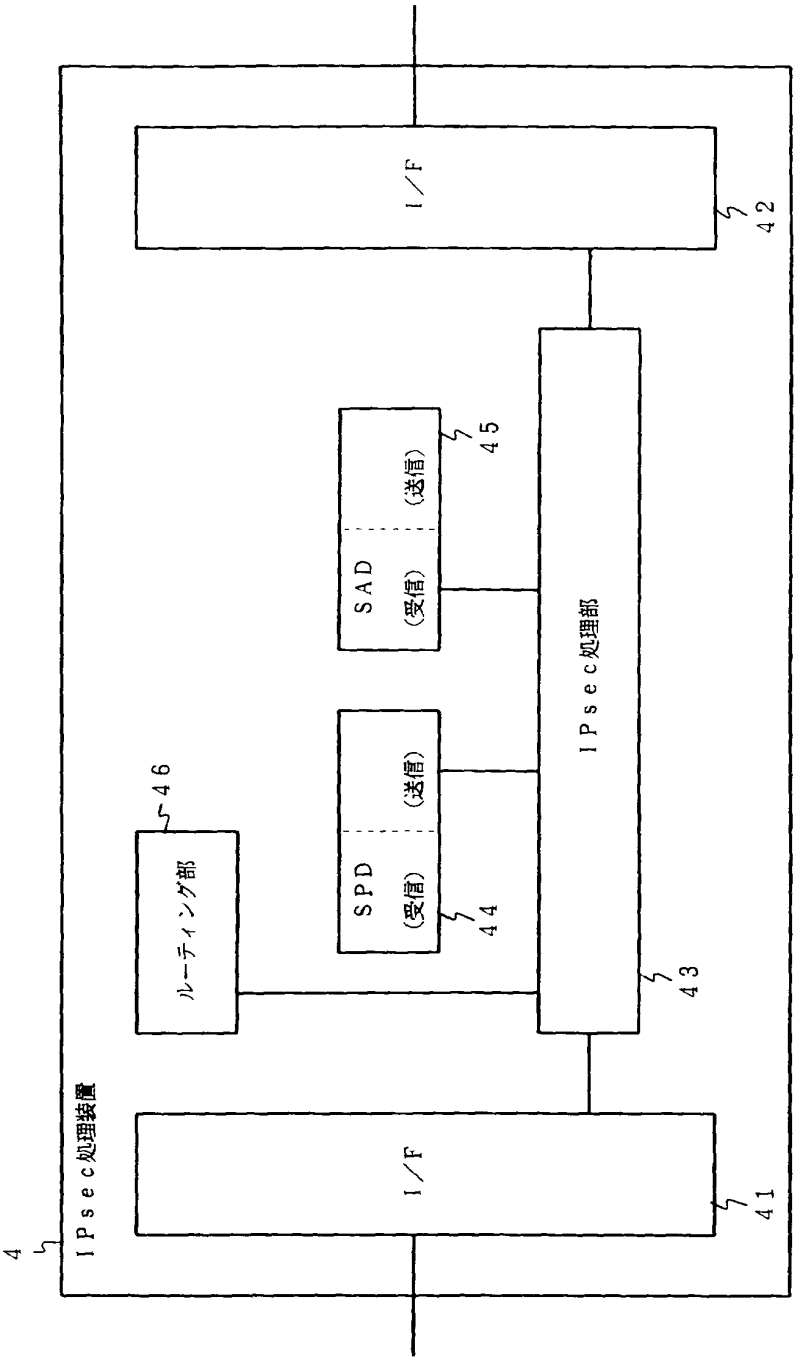
【図２９】


I／F
22
設定管理部
26
SAD
（受信）
（送信）
25
IPsec処理部
23
SPD
（受信）
（送信）
24
ルーティング部
27
上位
アプリケーション部
31
IPsec処理装置
3
28
記録媒体

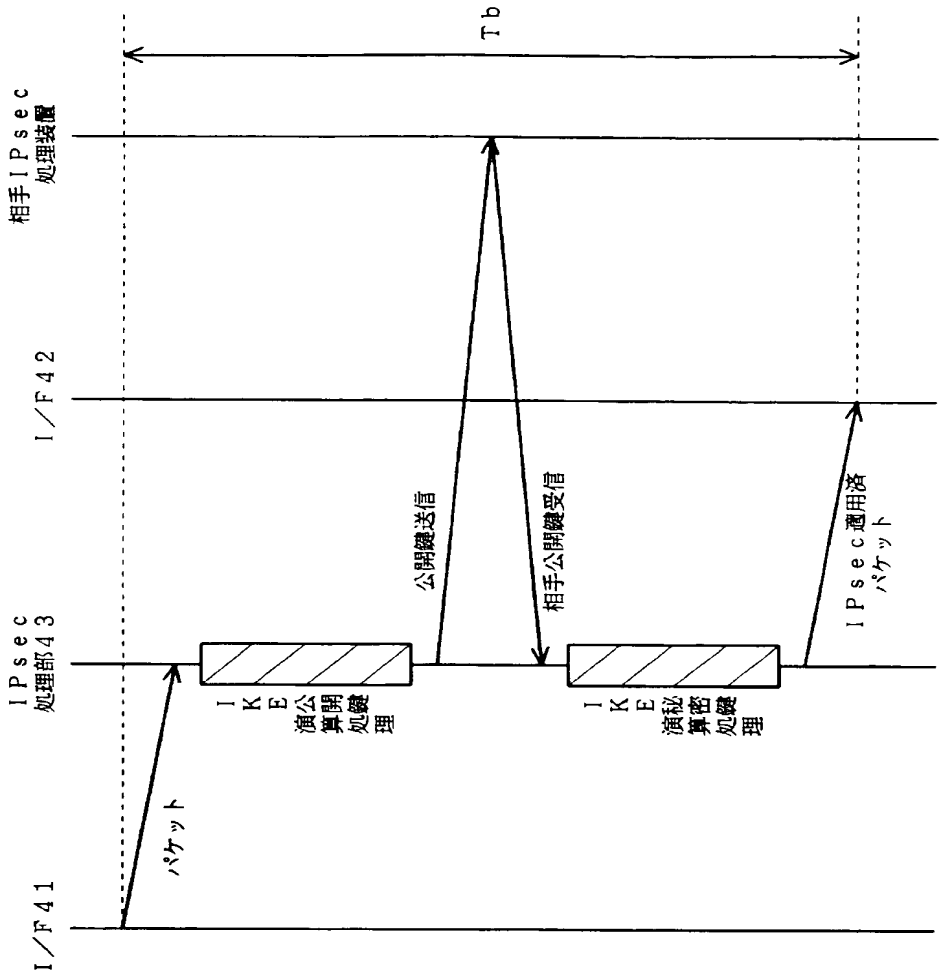
【図３０】


アドレスペア
配布ポリシー
ＩＰｓｅｃ処理装置２ｄ
ＩＰｓｅｃ処理装置２ｅ
ＩＰｓｅｃプロトコル　ＥＳＰ
カプセル化モード　トランスポートモード
暗号化アルゴリズム　３ＤＥＳ－ＣＢＣ
認証アルゴリズム　ＨＭＡＣ－ＳＨＡ－１－９６
ＳＡの有効期間　３６００秒
上記以外すべて
ＩＰｓｅｃプロトコル　ＥＳＰ
カプセル化モード　トンネルモード
暗号化アルゴリズム　ＤＥＳ－ＣＢＣ
認証アルゴリズム　ＨＭＡＣ－ＭＤ５－９６
ＳＡの有効期間　３６００秒
配布ポリシー（ｂ）
配布ポリシー（ａ）

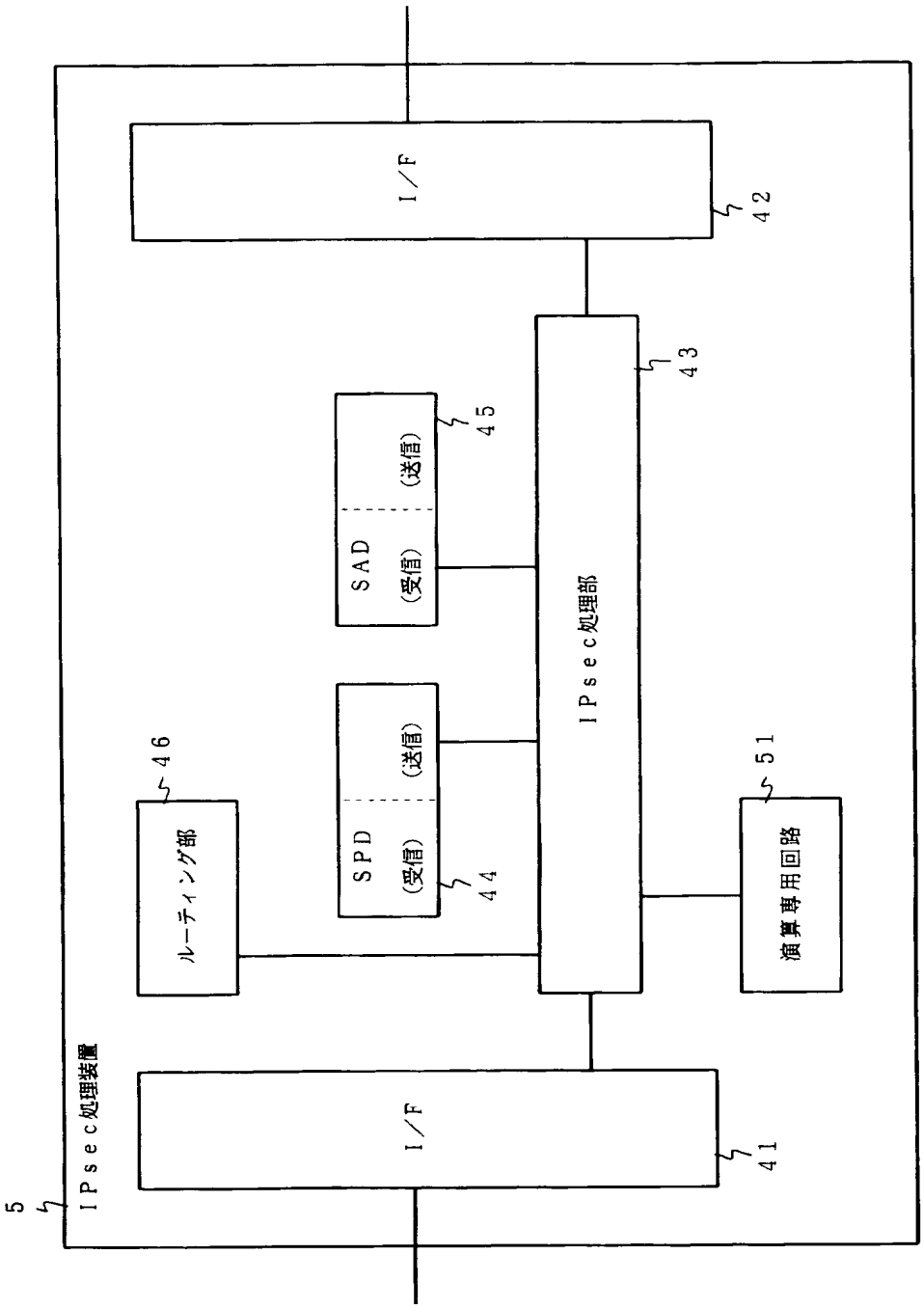
【図３１】


IPsec処理装置
4
I／F
41
ルーティング部
46
SPD
(受信)
(送信)
44
SAD
(受信)
(送信)
45
IPsec処理部
43
I／F
42

【図３２】


Tb
相手IPsec処理装置
I／F42
IPsec処理部43
I／F41
公開鍵送信
相手公開鍵受信
IPsec適用済パケット
パケット
IKE演算公開鍵処理
IKE演算秘密鍵処理

【図３３】


I／F
42
43
SAD
（受信）
（送信）
45
IPsec処理部
SPD
（受信）
（送信）
44
46
ルーティング部
51
演算専用回路
I／F
41
IPsec処理装置
5

【書類名】　　要約書

【要約】

【課題】　通信する装置間での設定不一致を防止可能なＩＰｓｅｃ設定サーバ装置を提供する。

【解決手段】　ＩＰｓｅｃ処理部１２はインタフェース部１１から受信したデータ通信パケットに対してＩＰｓｅｃ処理を実施する。ＳＰＤ１３はＩＰｓｅｃ処理部１２から参照され、ＩＰｓｅｃを適用するためのポリシーを記録している。ＳＡＤ１４はＩＰｓｅｃ処理部１２から参照され、個々の通信に対してＩＰｓｅｃ処理を実施するために必要なＳＡを記録している。要求処理部１５はＩＰｓｅｃ処理装置から設定要求メッセージを受信し、配布メッセージを返す。配布ポリシー記憶部１６は要求された設定を決定するために必要なＩＰｓｅｃポリシーが記憶されている。管理テーブル１７は設定要求を受けた各々のＳＡ通信に関する情報が記憶されている。

【選択図】　　図２

特願２００２－２６４９１３

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社